Mobile Administrator Manual

Spillman® Public Safety Software

Spillman Technologies, Inc.
4625 West Lake Park Blvd.
Salt Lake City, Utah 84120
Telephone: 1-800-860-8026
www.spillman.com

First Publication: August 2016

Notice

Table of Contents

Mobile Administrator Manual

Preface

Welcome to the *Mobile Administrator Manual.*

This manual is written for the Spillman Application Administrator (SAA) about how to set up and maintain the Mobile module.

This manual also contains setup and maintenance information for the following Mobile modules:

- Automated Field Reporting
- Driver License Scanning
- Local RMS Queries
- Mapping
- Messaging
- Premises Information
- State and National Queries
- Voiceless CAD

Using this manual

This manual contains the following information:

- Chapter 1 provides instructions for the basic setup and installation of Mobile, such as setting up the Mobile server and the Mobile client, and setting up the RMS Queries module and the Premises Information module.

- Chapter 2 provides instructions for setting up the following additional modules, including Driver License Scanning, Voiceless CAD, Mapping, and Automated Field Reporting. Instructions for using the Translation Administration Tool and the Field Manager are also provided.

- Chapter 3 provides instructions for monitoring and troubleshooting Mobile, and maintaining the Mobile Messenger module.

- Appendix A provides instructions on how to set up the Verified Entry feature.

Other manuals

The *Application Setup and Maintenance Manual* provides information for the Spillman Application Administrator (SAA) at your agency, including procedures for installing and maintaining Spillman Flex. The *Code Table Setup and Maintenance Manual* provides information for adding and maintaining your agency's code tables. The *Security Setup and Maintenance Manual* provides information for protecting your agency's system and setting up system privileges.

The following additional manuals contain setup information for modules that can be used with Mobile, but are not contained in this manual:

- *Automatic Vehicle Location (AVL) Manual*
- *Field Report and Forms Manual*
- *Quickest Route Manual*
- *State eCitation and State Crash Forms Manual*

Windows basics

Before using Mobile, be familiar with the standard features of Microsoft® Windows®. At a minimum, know how to do the following:

- Use a mouse or keyboard to perform basic tasks, such as choosing menu options and buttons
- Work with windows, such as selecting, minimizing, restoring, maximizing, sizing, scrolling, closing, and so forth
- Work with dialog boxes

If these tasks are unfamiliar, then refer to your Windows online documentation or complete an online Windows tour.

Manual conventions

When using this manual, note the following conventions.

Convention	Meaning/Use	Examples
bold	Used for names of options, text boxes, buttons, fields, and other items that appear on the screen.	**OK** is a button on the screen. Click **OK**, or press Enter.
angle bracket (>) between items	Shows the menu option(s) that must be selected, in sequence, to get to a specific option.	From the Start menu, select **All Programs** > **Spillman** > **Mobile**.
plus sign (+) between keys	Used for keys that are pressed at the same time. Hold down the first key, and then press the other key(s). When a keystroke is available for a mouse action, both the mouse action and the keystroke are presented.	Press Ctrl+E. Click **Close**, or press Ctrl+F4.
comma (,) between keys	Used for keys that are pressed in sequence. Press and release each key, in the order shown.	Press Alt, F, O to open the File Options dialog box.
`Courier font`	Used for displayed text. Used for table names.	The software prompts: `Are you sure you want to delete this record?` Open the Names table (`nmmain`).
`bold Courier font`	Used for information you enter.	Enter the street address, such as **`401 W Sycamore St`**.
italics	Used for emphasis. Used for variable information you supply.	Enter the date, using the *mm/dd/yyyy* format.

The following boxes indicate special information.

> **NOTE**
>
> Notes call attention to information that is of particular importance or that varies depending on a particular condition, such as the way your Spillman Application Administrator (SAA) has configured the software.

> **TIP**
>
> Tips present recommendations, optional actions, and additional ways to perform specific tasks.

> **CAUTION**
>
> Cautions point out actions that might endanger your data or its integrity (usefulness) or cause other problems later.

Features on your computer depend on your software version, modules, and privileges. Actual screens on your computer might vary from the example screens shown in this manual. However, any differences are minor and do not affect the tasks being described.

To find more manuals, visit MySpillman or the Spillman Knowlegebase.

Chapter 1

Installation and Setup

Jump to topic

Installing Mobile

Spillman Flex and Mobile are downloaded as one file. A Spillman Technologies Installation technician performs the initial Mobile installation. However, the Installation technician does not add new Mobile clients.

Adding new Mobile clients

To add a new Mobile client:

1. Navigate to the folder where the installation file is stored, and then double-click the `Spillman6.3 Full.exe` file to run the setup program.

   The Installation Wizard prepares the Windows Installer, and then the Client Setup screen opens.

2. Click **Next**.

Mobile Administrator Manual

The Setup Type screen opens.
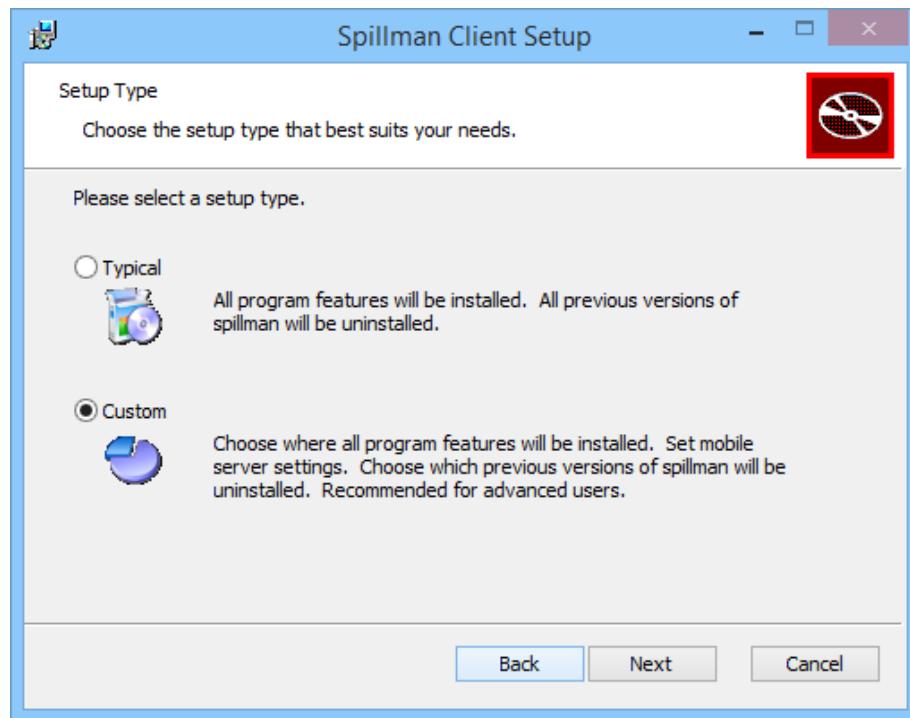
3. Do one of the following:

    – To install Spillman Flex with Mobile and uninstall any older versions of the software from your computer, select **Typical**. Continue to step 5.

    – To install Spillman Flex with Mobile and leave previous products installed, select **Custom**, and then click **Next**. The Products to Remove screen opens. Continue to step 4.

4. In the **Installed Products** area, highlight the product to remove, and then click **Add** to move it to the **Products to Remove** area. Repeat this step for all products that need to be uninstalled.

The selected products are listed in the **Products to Remove** area and are removed when the software is installed.
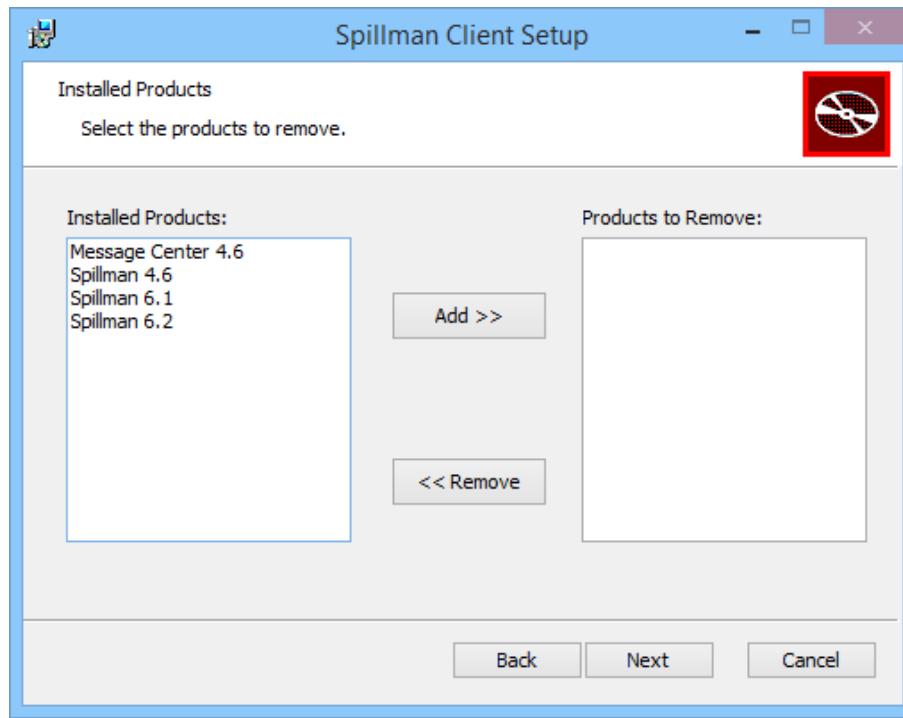
5. Click **Next**.

The Destination Folder screen opens, and the default destination folder is displayed.
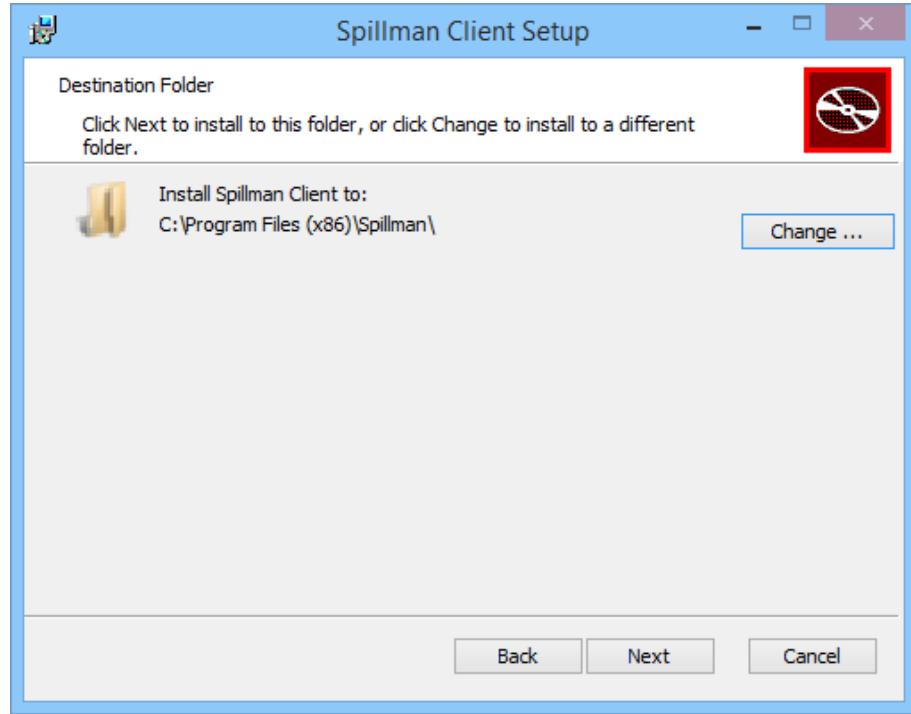
6. To change the destination folder, click **Change**, and then select a new location. Otherwise, click **Next**.

The Mobile Settings screen opens.
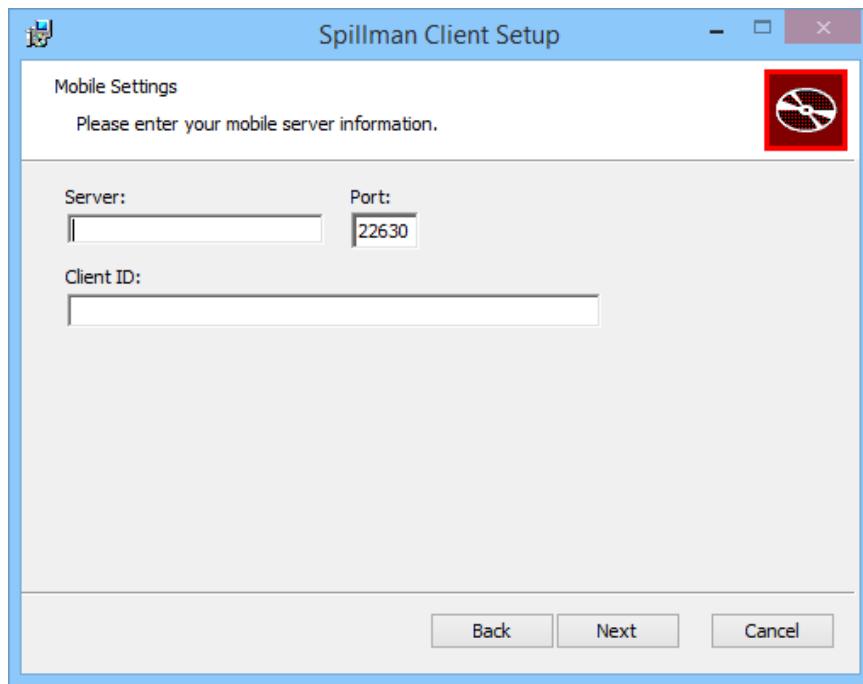
7. In the **Server** field, enter the IP address or domain name of the server that is running the software.

8. In the **Port** field, enter one of the following:

   – `22630` for the live database.

   – `22639` for the practice database.

9. If necessary, in the **Client ID** field, enter a Client ID. If your agency uses a dynamic IP network, then this field must be completed. For more information, see .

10. Click **Next**.

The Ready to Install the Program screen opens.
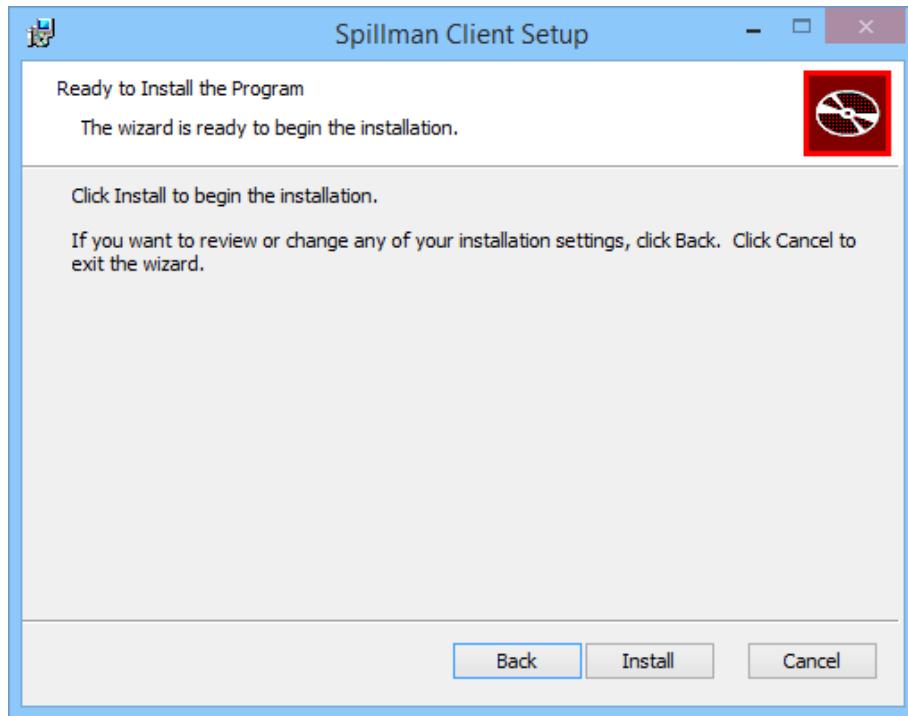
11. Click **Install** to continue installing the software. Click **Back** to return to the previous screen and change your settings.

    The software is installed and a message is displayed, advising of the completed installation.

12. Click **Finish** to exit the Installation wizard.

Upgrading Mobile

Mobile is automatically upgraded from the server at the same time as Flex. Mobile checks to see if any updated files or patches are available at startup. If updates are available, then the user is prompted to install them after logging in. For more information, see the *Mobile User Manual*.

Setting Up the Mobile Server

During the initial Mobile installation, a Spillman Installation technician defines the command that starts Mobile. The Dispatch server and the Mobile server are controlled by the `options.xml` file, which contains a set of XML tags that provides instructions for Mobile. Depending on your agency's needs, values of the XML tags can be changed. Encryption keys for all Mobile transactions must also be defined.

For StateLink 1.0 only, the message router is controlled by command line options, which are set up at the time of installation. For more information, see "Defining command line options" on page 20.

Defining command line options

For StateLink 1.0 only, the command line options listed in this section are for reference only. To modify the command line for Mobile, contact Spillman Technical Services.

The command line for the message router (`msgroutr`) uses the following format:

```
msgroutr -? or -help -d -expire minutes -junk directory
-no-log -no-xml -retry minutes -s port -v -wait directory
-x [host:]port -z
```

Command parameter	Description
`-?` or `-help`	Prints the command line parameters and exits the server. This command does *not* start the server.
`-d [level]`	Enables the debugging mode with options for level 0 and 1. Level 1 includes communication output debugging.
`-expire minutes`	Determines the number of minutes to wait before expiring a message. The default value is 120 minutes.
`-f`	Keeps processes in the foreground. If the -f option is omitted, then processes are kept in the background.
`-junk directory`	Determines the directory to which the router sends undeliverable messages.
`-L`	Forces all debugging to one file. If the `-L` (error logging) option is used when the server is started, all the server's output is stored in `$MOBILEDIR/log/22630/debug/server.trace`. If the `-L` option is not used when the server is started, then each client (unit) sends log entries to the client's log file after logging in. The file name uses the format `uIP-address.IP-address.trace`.

Command parameter	Description
`-no-log`	Turns off message logging in `ecrtrlog`. By default, message logging is enabled.
`-no-xml`	Determines the format, either XML or text, in which the protocol interface receives messages.
`-retry minutes`	Determines the number of minutes the message router waits before trying to resend a message. The default value is 10 minutes.
`-s port`	Defines the port number that the message router uses to communicate. The default value is 11400. **NOTE:** Mobile does not recognize port numbers above 35000. Use only port numbers below 35000.
`-v`	Prints the version number and exits the server. This command does *not* run the server.
`-wait directory`	Determines the directory in which the router puts messages to wait until they can be delivered.
`-x [host:][port]`	Determines the dispatcher connection settings. By default, the host is `localhost`, and the port is `12630`.
`-z`	Runs the message router in single-process mode (for debugging).

Accessing the options.xml file

The method used to access the `options.xml` file is based on your server's operating system. The file is modified using User Interface (UI) commands.

Windows users

For Windows users, navigate to the following directory:

`\\SpillmanServer\app\mobile\custom`

UNIX and Linux users

For UNIX and Linux users, complete the following:

1. At the command line, enter **sh**.

   The Terminal Emulator window opens.

2. At the prompt line, enter **cd $MOBILEDIR**.

   NOTE

   All commands are case sensitive.

3. At the prompt line, enter **cd custom**.

4. At the prompt line, enter the following:

```
vi options.22630.xml.
```

The `options.xml` file is displayed in the User Interface (UI) editor.

Defining XML tags for the Dispatch server

Settings for the Dispatch server are located in the `options.xml` file.
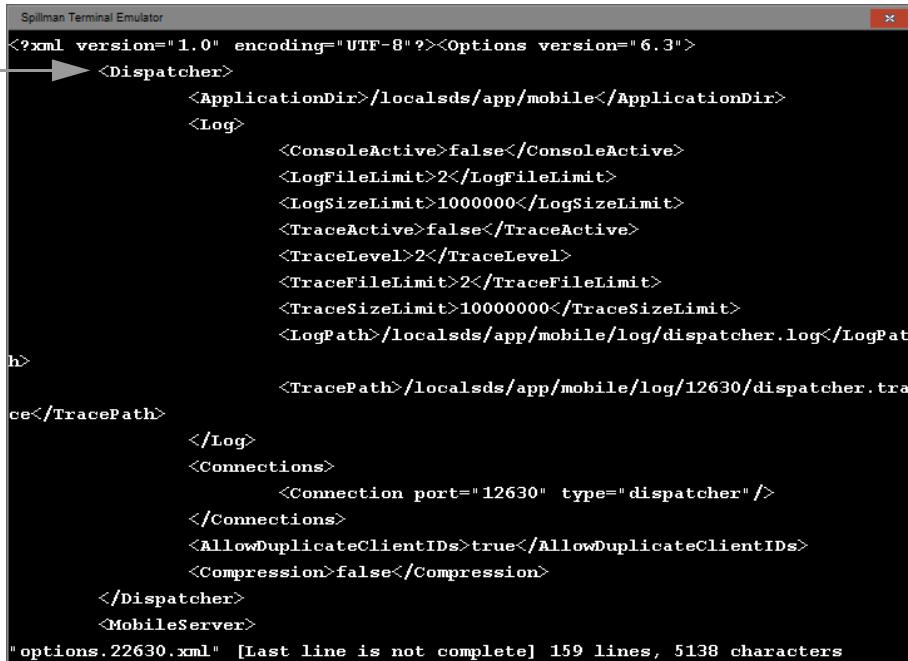
Dispatcher beginning
tag


```
Spillman Terminal Emulator
<?xml version="1.0" encoding="UTF-8"?><Options version="6.3">
        <Dispatcher>
                <ApplicationDir>/localsds/app/mobile</ApplicationDir>
                <Log>
                        <ConsoleActive>false</ConsoleActive>
                        <LogFileLimit>2</LogFileLimit>
                        <LogSizeLimit>1000000</LogSizeLimit>
                        <TraceActive>false</TraceActive>
                        <TraceLevel>2</TraceLevel>
                        <TraceFileLimit>2</TraceFileLimit>
                        <TraceSizeLimit>10000000</TraceSizeLimit>
                        <LogPath>/localsds/app/mobile/log/dispatcher.log</LogPat
h>
                        <TracePath>/localsds/app/mobile/log/12630/dispatcher.tra
ce</TracePath>
                </Log>
                <Connections>
                        <Connection port="12630" type="dispatcher"/>
                </Connections>
                <AllowDuplicateClientIDs>true</AllowDuplicateClientIDs>
                <Compression>false</Compression>
        </Dispatcher>
        <MobileServer>
"options.22630.xml" [Last line is not complete] 159 lines, 5138 characters
```

The following table describes the XML tags for the Dispatch server. The value shown in the table is the default value for the XML tag, unless otherwise noted.

Category	XML tag	Description
Dispatcher	`<Port>12630</Port>`	**NOTE:** This setting is no longer in use. Determines the dispatcher connection settings.
	`<ApplicationDir>D:/Spillman6.3/` `Mobile-6-3</ApplicationDir>`	Defines the server installation directory. If this tag is omitted, then the installation directory is determined automatically.
	`<MaxMessageQueueSize>15` `</MaxMessageQueueSize>`	**NOTE:** This setting is no longer in use. Determines the maximum number of messages allowed in the queue before the dispatcher sends content to the Mobile server client.

Category	XML tag	Description
Dispatcher > Log	`<ConsoleActive>false</ConsoleActive>`	Determines whether log files are sent directly to the console for debugging. **NOTE:** This tag should be modified by Spillman Technical Services only.
	`<LogFileLimit>2</LogFileLimit>`	Determines the number of rotating log files. After the `LogSizeLimit` is reached, the software creates a new log file. After the `LogFileLimit` is reached, the software overwrites the first log file.
	`<LogSizeLimit>1000000</LogSizeLimit>`	Determines the maximum size (in bytes) to which a log file can grow.
	`<TraceActive>false</TraceActive>`	Enables tracing functionality.
	`<TraceLevel>0</TraceLevel>`	Enables debugging mode and specifies the trace level. Enter one of the following: • **0**: Normal • **1**: Includes communication output. • **2**: Includes timers and updates.

Category	XML tag	Description
	`<TraceFileLimit>2</TraceFileLimit>`	Determines the number of rotating trace files. After the `TraceSizeLimit` is reached, a new trace file is created. After the `TraceFileLimit` has been reached, the first trace file is overwritten.
	`<TraceSizeLimit>10000000 </TraceSizeLimit>`	Determines the maximum size (in bytes) to which a trace file can grow.
	`<LogPath>D:/Spillman6.3/Mobile-6-3/log/126 30/dispatcher.log</LogPath>`	Defines the path for the log file. This path must be defined for logging to work. If your agency uses rotating log files, then the log files are named using the following format: *filenameN*`.log` where *filename* is the name of the log file, and *N* is the number of the log file in the rotation. For example, `dispatcher0.log`, `dispatcher1.log`.
	`<TracePath>D:/Spillman6.3/ Mobile-6-3/log/12630/dispatcher .trace</TracePath>`	Defines the path for the trace file. The path must be defined for logging to work. If your agency uses rotating log files, then the log files are named using the following format: *filenameN*`.trace` where *filename* is the name of the trace file, and *N* is the number of the trace file in the rotation. For example, `dispatcher0.trace`, `dispatcher1.trace`.
`Dispatcher > Connections` **NOTE:** The value shown in this XML tag is an *example* value.	`<ConnectionPort="12630" type="dispatcher"/>`	Determines the dispatcher connection settings. **NOTE:** Mobile does not recognize port numbers above 35000. Use only port numbers below 35000.

Category	XML tag	Description
Dispatcher	`<AllowDuplicateClientIDs>true</AllowDuplicateClientIDs>`	Prevents multiple users from logging on with the same client ID. • Set to **true** to allow multiple users log on with the same client ID. • Set to **false** to prevent multiple users from logging on with the same client ID. The default value is `true`.
	`<Compression>false</Compression>`	Determines if data compression is enabled, which minimizes the size of the files transferred between the Dispatch server and the computers running Mobile. • Set to **true** to enable compression. • Set to **false** to disable compression. By default, the value is `false`.

Defining XML tags for the Mobile server

Settings for the Mobile server are located in the `options.xml`file.

Dispatcher end tag
MobileServer begin tag

```
Spillman Terminal Emulator
                      <Compression>false</Compression>
                 </Dispatcher>
                 <MobileServer>
                      <ServicePort>22630</ServicePort>
                      <Compression>true</Compression>
                      <Encryption>false</Encryption>
                      <DynamicORIs>false</DynamicORIs>
                      <RadioLogHistoryHours>8</RadioLogHistoryHours>
                      <LocalSearchResultsMaximum>60</LocalSearchResultsMaximum>
                      <ExternalPasswordCheck>false</ExternalPasswordCheck>
                      <State>fl</State>
                      <BindToAddress>true</BindToAddress>
                      <XCurServer>
                           <Host>localhost</Host>
                           <Port>893</Port>
                           <AuthenticationTimeout>15</AuthenticationTimeout>
                      </XCurServer>
                      <AVL>
                           <Log>false</Log>
                           <GPSDisplay>
                                <MapCallPosition>true</MapCallPosition>
                                <MapUnitPosition>true</MapUnitPosition>
                                <ProcessUnitPosition>true</ProcessUnitPosition>
```

The following table describes the XML tags for the Mobile server. The value shown is the default value for the XML tag, unless otherwise noted.

Category	XML tag	Description
MobileServer	`<ServicePort>22630</ServicePort>`	Defines the port number that Mobile uses to communicate or the service name that is defined in the `/etc/services` files. **NOTE:** Mobile does not recognize port numbers above 35000. Use only port numbers below 35000.
	`<Compression>true</Compression>`	Disables data compression, which minimizes the size of the files transferred between the Mobile server and the computers running Mobile. • Set to **true** to enable data compression. • Set to **false** to disable data compression. By default, the value is `true`.

Category	XML tag	Description
	`<Encryption>true</Encryption>`	Disables 128-bit encryption. • Set to **true** to enable encryption. • Set to **false** to disable encryption. By default, the value is `true`.
	`<DynamicORIs>false</DynamicORIs>`	Dynamically assigns Originating Reporting Identifiers (ORIs). • Set to **true** to enable dynamic ORI assignment. • Set to **false** to disable dynamic ORI assignment. This option is available only if CAD is enabled. By default, the value is `false`.
	`<RadioLogHistoryHours>8` `</RadioLogHistoryHours>`	Determines the maximum number of hours for which the software can retrieve radio log entries. The value set by users in the Options dialog box cannot be greater than the `RadioLogHistoryHours` value. This option is available only if CAD is enabled.
	`<LocalSearchResultsMaximum>60` `</LocalSearchResultsMaximum>`	Defines the maximum number of records to return in response to a local search.
	`<State/>`	Defines the state abbreviation for state-specific features. For example, enter **UT** for Utah. By default, this tag is blank.
	`<ClientIDFullIPAddress>false` `</ClientIDFullIPAddress>`	Determines whether the Mobile Client ID uses the last two octets of the IP address separated by a colon, or the full IP address. • Set the value to **true** to use the full IP address. • Set the value to **false** to use only the last to octets separated by a colon. By default, the value is `false`.

Category	XML tag	Description
	`<DNSNameResolutionTimeout>10` `</DNSNameResolutionTimeout>`	Determines the time (in seconds) that the Mobile server will wait before terminating the function call. If a server times out, then the client's workstation identifier is set to the IP address, instead of the resolved host name. This option is automatically added to the `options.xml` file upon Mobile server startup. The default setting is `10` (seconds), which is the recommended setting.

`MobileServer >`
`XCurServer`
NOTE: The values shown in these XML tags are *example* values.
	`<Host>localhost</Host>`	Specifies the server on which XCurServer runs.

	`<Port>893</Port>`	Specifies the port on which XCurServer runs. **NOTE:** Mobile does not recognize port numbers above 35000. Use only port numbers below 35000.
	`<AuthenticationTimeout>15` `</AuthenticationTimeout>`	Specifies the amount of time (in seconds) the Mobile Server will attempt to communicate successfully with XCurServer before it times out. By default, the value is `15` (seconds), which is the recommended setting.
`MobileServer >` `AVL`	`<Log>false</Log>`	**NOTE:** This setting is no longer in use. Enables AVL logging. • Set to **true** to enable logging. • Set to **false** to disable logging. By default, the value is `false`.

`MobileServer >`
`AVL > GPSDisplay`
NOTE: These options are available only if AVL is enabled.
	`<MapCallPosition>true`
	`</MapCallPosition>`
		Determines whether CAD calls are shown on the map.
		• Set to **true** to show CAD calls on the map.
		• Set to **false** hide CAD calls from the map.
		By default, if the AVL and Mapping modules are enabled, then the value is set to `true`.

Category	XML tag	Description
	`<MapUnitPosition>true </MapUnitPosition>`	Determines whether units are shown on the map. • Set to **true** to show units on the map. • Set to **false** hide units from the map. By default, if the AVL and Mapping modules are enabled, then the value is set to `true`.
	`<ProcessUnitPosition>true </ProcessUnitPosition>`	Determines whether the server processes AVL information from units. • Set to **true** to process AVL information from units. • Set to **false** to not process AVL information from units. By default, if the AVL and Mapping modules are enabled, then the value is set to `true`.
`MobileServer > AVL > GPSUpdates` **NOTE:** These options are available only if AVL is enabled.	`<Distance>300</Distance>`	Determines the maximum distance (in meters) that a unit can travel before the position of the unit is updated.
	`<Maximum>60</Maximum>`	Determines the maximum number of seconds to wait before updating the position of a unit.
	`<Minimum>5</Minimum>`	Determines the minimum number of seconds to wait before updating the position of a unit.
	`<NoAVLOnCode/>`	Determines if a unit stops reporting GPS coordinates, based on the status of the unit. Enter a `tb10code` value that identifies when a unit should stop reporting GPS coordinates. By default, the value is blank.
`MobileServer > AVL > QuickestRoute` **NOTE:** These options are available only if Quickest Route is enabled.	`<DistanceDeviation>50 </DistanceDeviation>`	Determines the distance (in meters) at which routing information is regenerated after a device goes off course.

Category	XML tag	Description
	`<TimeManeuver>30</TimeManeuver>`	Determines the time (in seconds) at which the maneuver icons in the **Directions** pane change to show the next maneuver.
	`<RouteUpdateMinimum>30 </RouteUpdateMinimum>`	Determines the length of time (in seconds) the software waits before updating a route.
	`<RouteUpdateMaximum>300 </RouteUpdateMaximum>`	Determines the length of time (in minutes) the software waits to request a new route for a stationary unit.
	`<RouteUpdateDistance>300 </RouteUpdateDistance>`	Determines the distance (in meters) a unit travels before the software requests an updated route. This setting works in conjunction with the `RouteUpdateMinimum` option. When the `RouteUpdateDistance` value has been reached, the software then fulfills the `RouteUpdateMinimum` value. For example, if `RouteUpdateMinimum` is set to `1` (second), and `RouteUpdateDistance` is set to `1` (meter), then after the unit has traveled one meter, the software will request a new route after one second.
`MobileServer > CADAggregator`	`<AggregatorUpdates>10 </AggregatorUpdates>`	**NOTE:** This setting is no longer in use. Determines the refresh rate of CAD aggregation. Keep this number lower than the `Client > BandwidthControl > CADUpdates` setting.

Category	XML tag	Description
	`<Enabled>true</Enabled>`	**NOTE:** This setting is no longer in use. Determines if the CAD Aggregator is enabled. If your agency is in the process of migrating to a new Mobile version, and both versions are running simultaneously, then disable one of the aggregators so that only one aggregator is running. • Set to **`true`** to enable the CAD aggregator. • Set to **`false`** to disable the CAD aggregator. By default, the value is `true`.
	`<ResetTables>true</ResetTables>`	**NOTE:** This setting is no longer in use. Determines if the aggregator tables are removed and restored at startup. • Set to **`true`** to remove and restore the aggregator tables at startup. • Set to **`false`** to not remove and restore the aggregator tables at startup. By default, the value is `true`. **NOTE:** Do not set the value to `false` unless instructed by Spillman Technical Services.

`MobileServer >`
`Client >`
`BandwidthControl`
	`<MaximumDeadAir>60</MaximumDeadAir>`	Determines the maximum number of minutes a Mobile session can run without communication with the server before the session is ended.

	`<MaximumInactivity>120` `</MaximumInactivity>`	Determines the maximum number of minutes a Mobile session can be inactive before the session is ended.
	`<CADUpdates>15</CADUpdates>`	Determines how often (in seconds) the server updates the calls in Voiceless CAD and Mobile Mapping. This option is available only if CAD is enabled.

Category	XML tag	Description
	`<UnitUpdates>30</UnitUpdates>`	Determines how often (in seconds) the server updates the units in Voiceless CAD and Mobile Mapping. This option is available only if CAD is enabled.
	`<CADUnitActivity>14 </CADUnitActivity>`	Determines the number of days a unit can go without updating the server before being removed from the list of units in Voiceless CAD. This option is available only if CAD is enabled.
	`<GPSUpdates>30</GPSUpdates>`	Determines how often (in seconds) the device sends location information to the server. This option is available only if AVL is enabled.
	`<WorkflowUpdates>60 </WorkflowUpdates>`	Determines how often (in seconds) the server checks for new Workflow messages. This option is available only if the Workflow Management feature is enabled.
	`<DispatcherReconnect>60 </DispatcherReconnect>`	Determines how often (in seconds) the Mobile server tries to reconnect with the Dispatch server if the connection is lost.
	`<ContactsUpdates>30</ContactUpdates>`	Determines how often (in seconds) the server sends new contact listings.
	`<ClientPingInterval>0 </ClientPingInterval>`	Determines how often (in seconds) the Mobile server pings (sends an empty message to) the client. For example, to set the Mobile server to ping the client once every minute, set the value to `60`. This setting keeps communication between the client and the server active. The `ClientPingInterval` option is only required for some unusual network configurations.

Category	XML tag	Description
	`<MessageCenterUpdates>120 </MessageCenterUpdates>`	**NOTE:** This setting is no longer in use. Determines how long (in seconds) Mobile waits between searching for and sending undelivered messages. This allows messages to be sent, even when the dispatcher is down.
`MobileServer > Client > SupportedClient Builds`	`<Minimum>45</Minimum>`	**NOTE:** This setting is no longer in use. Determines the minimum build version a user must have to log in to Mobile.
	`<Maximum>45</Maximum>`	**NOTE:** This setting is no longer in use. Determines the maximum build version a user must have to log in to Mobile.
`MobileServer > Client`	`<WarnDuplicateClient>true </WarnDuplicateClient>`	Determines if a warning message is displayed in Mobile and the Message Center when a user is logged in with a client ID that another user also used to log in. • Set to **true** to display the warning message. • Set to **false** to not display the warning message. By default, the value is `true`.
	`<AutoFileSyncSize>0 </AutoFileSyncSize>`	Specifies the total size (in kilobytes) that will be automatically downloaded when Mobile retrieves the available downloads on startup. If the total size is less than the number specified in `AutoSyncFileSize`, then the files download automatically and no prompt is displayed.
	`<DraftAutoSaveTimeOut>30 </DraftAutoSaveTimeOut>`	Determines how often (in seconds) a draft is saved when changes are made to a form. This setting applies to all forms created in Mobile.

Mobile Administrator Manual

Category	XML tag	Description
	`<NovoCacheCapSize>30</NovoCacheCapSize>`	Determines the maximum number of items cached per search type. Once the maximum number of items are cached, the oldest items are removed so that the cache stays at the specified value as additional searches are performed. This setting affects anything in Mobile that relies on previous search data, such as the Mobile Field Report and the State Crash and State eCitiation forms. For example, if the value is set to `30`, then in the Mobile Field Report, in the **Persons** tab, in the Recent Searches list, up to 30 of the most recent Name records searched in Mobile are displayed.
	`<NovoStateLinkNameCasing>Upper</NovoStateLinkNameCasing>`	Determines whether a StateLink return is uppercase, lowercase, or mixed case when the return is imported. Set to one of the following values: • `Upper`: Changes imported text to uppercase. • `Lower`: Changes imported text to lowercase. • `THank`: Changes imported text to mixed case. By default, the value is `Upper`.
	`<NovoUpdateVehicleOwner>true</NovoUpdateVehicleOwner>`	Determines whether the owner of a vehicle will be automatically populated in the State Crash or State eCitation forms when a vehicle is selected for the form. • Set to `true` to automatically populate the owner of a vehicle. • Set to `false` to not automatically populate the owner of a vehicle. By default, the value is `true`.

Category	XML tag	Description
	`<NovoDisableOfflineMode>false </NovoDisableOfflineMode>`	Enables limited operation in Mobile if the client loses connection with the server. • Set to **`true`** to disable Offline mode. If Offline mode is disabled, then offline records cannot be created. • Set to **`false`** to enable Offline mode. If Offline mode is enabled, then offline records can be created. By default, the value is `false`, and offline records can be created.
	`<NovoConfirmInvalidSubmission>false <NovoConfirmInvalidSubmission>`	Determines if an error message is displayed when validation for a form fails. • Set to **`true`** to display an error message when validation fails. • Set to **`false`** to not display an error message when validation fails. By default, the value is `false`.
	`<ERSUrl/>`	Determines the ERS website linked to Mobile. By default, this tag is not listed and needs to be entered only if the ERS link stops working.
`MobileServer > CadWebAggregator`	`<Port>17777</Port>`	Specifies the port on which the CAD Web Aggregator runs. **NOTE:** Mobile does not recognize port numbers above 35000. Use only port numbers below 35000.
	`<Host>localhost</Host>`	Specifies the server on which the CAD Web Aggregator runs.
`MobileServer > Imaging`	`<Directory>/images/</Directory>`	**NOTE:** This setting is no longer in use. Defines the path to the **Images** folder.

Category	XML tag	Description
`MobileServer >` `SSL`	`<Certificate>spillman.cert` `</Certificate>`	Displays the name of the certificate that Mobile uses when encryption is enabled. **NOTE**: Do not modify this value unless instructed by Spillman Technical Services.
	`<PrivateKey>spillman.pem</PrivateKey>`	Displays the name of the private key that Mobile uses when encryption is enabled. **NOTE**: Do not modify this value unless instructed by Spillman Technical Services.
`MobileServer >` `XMLDServer` **NOTE:** The values shown in these XML tags are *example* values.	`<Host>192.168.1.2</Host>`	Specifies the server on which the Data Exchange runs.
	`<Port>9000</Port>`	Specifies the port on which the Data Exchange runs. **NOTE:** Mobile does not recognize port numbers above 35000. Use only port numbers below 35000.
`MobileServer >` `Forms`	`<ServerCache>false</ServerCache>`	Determines whether a copy of the Standard Storage Format File (`.ssf`) is cached when a form is saved. **NOTE:** This setting applies to the PDF forms only, and should only be used if the forms or drafts are not saving correctly. Contact Spillman Technical Services before changing this setting.
	`<DaysToCache>14</DaysToCache>`	Determines how many days an `.ssf` file should be cached, if `ServerCache` is enabled. **NOTE:** This setting applies to the PDF forms only, and should only be used if the forms or drafts are not saving correctly. Contact Spillman Techincal Services before changing this setting.

Category	XML tag	Description
	`<BackupDrafts>false</BackupDrafts>`	Determines if a backup file for the draft is created. **NOTE:** This setting applies to the PDF forms only, and should only be used if the forms or drafts are not saving correctly. Contact Spillman Techincal Services before changing this setting.
	`<DaysToBackup>14</DaysToBackup>`	Determines how many days the backup file is saved, if `BackupDrafts` is enabled. **NOTE:** This setting applies to the PDF forms only, and should only be used if the forms or drafts are not saving correctly. Contact Spillman Techincal Services before changing this setting.
	`<IsVerifiedEntryEnabled>false</IsVerifiedEntryEnabled>`	Determines if the Verified Entry feature is used at a World level when adding new records to Mobile. For more information, see "Setting up the Verified Entry setting" on page 163. **NOTE:** For most agencies, this setting is not needed, and does not need to be modified from the default.
`MobileServer > GenericLaw`	`<WhenReported>2 WKS</WhenReported>`	Determines the default search period for Law Incident records when completing a new Mobile Field Report. For more information, see the *Mobile Field Report and Field Interview Manual*.
`MobileServer > TraCS`	`<Active>false</Active>`	Determines if state returns for TraCS are placed in a location on the client to be used by other applications. • Set to **true** to place TraCS state returns in a specified file location to be used by other applications. • Set to **false** to not place TraCS state returns in a specified file location to be used by other applications. By default, the value is `false`.

Category	XML tag	Description
	`<MessageCache>C:\TraCS\MessageCache</MessageCache>`	Defines the path to the file location on which the TracCS state returns are placed, if the `MobileServer > TraCS > Active` setting is set to `true`.
`MobileServer > InSight` **NOTE:** These options are available only if InSight is enabled. The values shown in these XML tags are *example* values.	`<Host>insight.agency.gov</Host>`	Defines the name of the InSight host.
	`<Port>8080</Port>`	Defines the InSight web service port. **NOTE:** Mobile does not recognize port numbers above 35000. Use only port numbers below 35000.
	`<NotifyPort>4445</NotifyPort>`	Defines the InSight notify port.
	`<Timeout>5</Timeout>`	Determines how long (in seconds) Mobile waits for a response from the InSight server when a user logs in to Mobile. If a connection is not made within the specified time frame, Mobile stops trying to make a connection.
	`<RepsonseTimeout>5</ResponseTimeout>`	Determines how long (in seconds) Mobile waits for a response from the Insight server when a query is performed. If a response is not received within the specified time frame, then an error is displayed.
`MobileServer > StateLink > Locations`	`<Path>D:/Spillman6.3/Mobile-6-3/ interfaces-server/webapps/StateLinkST </Path>`	Defines the path for the StateLink 2.0 client files.
`MobileServer > StateLink` **NOTE:** The values shown in these XML tags are *example* values.	`<Host>localhost</Host>`	Specifies the server on which StateLink 2.0 runs.
	`<Port>5555</Port>`	Defines the port on which StateLink 2.0 runs. **NOTE:** Mobile does not recognize port numbers above 35000. Use only port numbers below 35000.
	`<Version>2</Version>`	Defines which version of StateLink is being used.

Category	XML tag	Description
MobileServer > Log	`<TraceActive>false</TraceActive>`	Enables or disables debugging mode.
	`<TraceLevel>0</TraceLevel>`	Specifies the debugging level. Use one of the following values: • `0`: Normal • `1`: Includes communication output. • `2`: Includes timers and updates.
	`<TraceConsolidateFile>false </TraceConsolidateFile>`	Determines whether the server writes all error logging and debuging information to one file. • Set to **`true`** to write all error logging and debugging information to one file. • Set to **`false`** to write debugging and logging information to separate files, based on the unit ID. By default, the value is `false`.
MobileServer > MiddleTier	`<Connect>false</Connect>`	**NOTE:** This option is no longer in use. Determines whether the Mobile server connects to MiddleTier.
	`<DatabaseAdapter>live </DatabaseAdapter>`	**NOTE:** This option is no longer in use. Enter the name of the database from which MiddleTier obtains data. By default, the database name is `live`.

Category	XML tag	Description
MobileServer > Alerts	`<FilterNonAgencyAlerts>false </FilterNonAgencyAlerts>`	Determines whether the software sends alerts to all administrators. • Set to **`true`** to alert only those administrators who are members of the groups receiving the alert. • Set to **`false`** to alert all administrators. By default, the value is `false`. **NOTE:** The user who sent the alert will see the alert regardless of the groups to which the user is assigned.
	`<EmergencyAlertsToAllAgencies>false </EmergencyAlertsToAllAgencies>`	Determines whether the software sends Emergency Alerts to all agencies. • Set to **`true`** to alert all agencies on the server. • Set to **`false`** to alert only the agency of the user who sent the alert. By default, the value is `false`.
MobileServer > CAD	`<AssignDefaultStatus>ENRT </AssignDefaultStatus>`	Determines the default unit status when the Assign Self to Call feature is used. Enter the desired default status between the beginning and ending tags.
	`<NewCallDefaultNature>TrafficOffense </NewCallDefaultNature>`	Determines the default call nature the first time the Add a New Call Record screen is opened in Mobile. However, if a different nature is selected, then the next time the Add a New Call Record screen is opened, the last selected nature is used to complete the field. Enter the desired default nature between the beginning and ending tags.
	`<NewCallDefaultStatus>ENRT </NewCallDefaultStatus>`	Determines the default unit status when the Add A CAD Call feature is used. Enter the desired default status between the beginning and ending tags.

Category	XML tag	Description
	`<OnSiteDefaultNature>TrafficOffense</OnSiteDefaultNature>`	Determines the default call nature when the On Site Call feature is used. Enter the desired default nature between the beginning and ending tags.
	`<OnSiteDefaultStatus>ARRVD</OnSiteDefaultStatus>`	Determines the default unit status when the On Site Call feature is used. Enter the desired default nature between the beginning and ending tags.

Synchronizing client files

A file synchronization check is performed on the Mobile client machine automatically each time a user logs in to Mobile. If there is information on the client that is not found on the Mobile server, then the software removes the files from the client machine. To keep the downloaded directories for a client machine, the files must be saved on the Mobile server.

Encrypting Mobile Transactions

Criminal Justice Information Sharing (CJIS) requirements mandate that approved encryption methods be used on any portion of a network that is not wholly owned by law enforcement. This applies to all mobile applications that run over public wireless networks.

CJIS security requirements mandate that law enforcement agencies use a secure criminal justice information system.Ways of meeting the CJIS encryption requirement include the following:

- **The built-in encryption provided with your software.** This method is certified by the Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST). The built-in encryption is for data transmitted between the server and all client software. The encryption must be enabled to be used. For more information, see the *CJIS Compliance Administrator Guide* and FIPS PUB 140-2.

> **NOTE**
>
> If a new encryption certificate is needed, then contact Spillman Technical Services for assistance.

- **A Virtual Private Network (VPN).** The VPN must use an encryption methodology to protect Mobile communication and all other applications. VPN software uses Advanced Encryption Standard (AES) to meet the required encryption method and is certified by the NIST.

> **NOTE**
>
> If your agency is using the Mobile Multi-Server system, then to meet the CJIS encryption requirement, a VPN must be used. The built-in encryption provided with your software is not available for multi-server systems.

Setting Up the Mobile Client

This section describes the general setup tasks that must be completed for all Mobile modules. For the Mapping, State and National Queries, and Voiceless CAD modules, additional administrative tasks must be completed. After the general setup tasks are completed, refer to "Setting Up Mobile Modules" on page 69 for module-specific tasks.

For information on how to set up privileges for individual users and groups of users, see the *Security Setup and Maintenance Manual*.

Using PassKey

If your agency uses the PassKey feature to securely log in to Mobile, in addition to the user name and password, then for information on setting up PassKey, see the *CJIS Compliance Administrator Guide*.

Setting up system privileges for Mobile

Specify which Mobile modules and administrative features users can access. If the privileges for a user are changed while the user is logged in to Mobile, then the user must close Mobile and log back in for the changes to take effect.

Giving a user basic access

The following table lists all the modules to which access can be granted or restricted.

> **NOTE**
>
> Access can be granted to only those modules that your agency has purchased, so some of the privileges in the following table might not apply to your agency.
>
> This list is not all-inclusive. For information on granting access to a module not listed in this table, see the manual for that module.

Module	System Privilege	Description	Privilege
Automated Field Reporting **NOTE**: These privileges are for the PDF forms only. To set up the Mobile Field Report, see the *Mobile Field Report and Forms Manual*. To set up the State Crash and State eCitation forms, see the *State eCitation and State Crash Forms Manual*.	`mdcmdlafracc`	Grants access to the General Use Accident form.	Access
	`mdcmdlafrcit`	Grants access to the General Use Incident form.	Access
	`mdcmdlafrfi`	Grants access to the General Use Field Interview form.	Access
	`mdcmdlafrfrfi`	Grants access to the General Use Fire Field Interview form.	Access
	`mdcmdlafrlaw`	Grants access to the General Use Law form.	Access
	`mdcmdlafrwarn`	Grants access to the General Use Warning form.	Access
	`mdcmdlstforms`	Grants access to the State Forms module in Mobile.	Access
Driver License Scanning	`mdcmdldlscan`	Allows the user to swipe or scan driver licenses.	Access
ERS	`mdcmdlers`	Grants access to the ERS interface.	Access
File Management	`fileadmin`	Grants access to the File Capture window and manage files.	Access
	`filecapture`	Grants access to the File Capture window, manage files, and see form attachments in workflow.	Access
	`hidefiles`	Grants the ability to hide files.	Access
InSight Queries	`mdcmdlinsight`	Enables the InSight search options on Mobile query screens.	Access

Module	System Privilege	Description	Privilege
Mapping	`mdcmdlcllcomment`	Enables the **Call Comments** button on the Mobile Mapping screen.	Access
	`mdcmdlmapping`	Grants access to the Mapping screen.	Access
	`mdcmdlqroute`	Enables the **Quickest Route** button on the toolbar.	Access
Messaging	`mdcmdlemergency`	Enables the **Emergency Alert** button on the toolbar.	Access
	`mdcmdlim`	Grants the ability to send and receive instant messages, and use all send/receive features.	Access
	`mdcmdlimext`	Grants the ability to add an external (non-Mobile) user to IM and Message groups.	Access
	`mdcmdlmsging`	Grants the ability to send and receive messages, and use all send/receive features.	Access
Pictometry	`mdcmdlpictometry`	Grants access to the Pictometry interface.	Access
Premises Information	`mdcmdlpremises`	Grants the ability to query the database from the Premises and HazMat screens, and to view the **Premises** and **HazMat** tabs on the CAD screen.	Access
RMS Queries	`mdcmdllocquery`	Grants the ability to query your agency's local database.	Access
Voiceless CAD	`mdcmdlcad`	Grants access to the Voiceless CAD module, which includes the CAD screen, Radio Log History screen, Unit Status screen, and Radio Log dialog box.	Access
	`mdcmdlnewcall`	Grants the ability to add a call using the **New Call** button.	Access, Modify
	`mdcmdloscall`	Grants the ability to add a call using the On-Site Call button.	Access, Modify
Workflow Management	`mdcmdlworkflow`	Grants the ability to track and update the status of records.	Access

Module	System Privilege	Description	Privilege
Various modules	`cdcall`	Grants the ability to use the CAD Call Search screen.	Access
	`cpmain`	Grants access to the Civil Process Search screen.	Access
	`ctmain`	Grants access to the Citation Search screen.	Access
	`dsmain`	Grants access to the Dissemination Search screen.	Access
	`emmain`	Grants access to the EMS Search screen.	Access
	`evmain`	Grants access to the Evidence Search screen. Gives users access to the **Evidence** check box and **Evidence** tab in Mobile records. In Flex, gives users access to the Evidence Management table. Users who add evidence items, scan barcodes, or use the **Cust** button must be given access to the screen.	Access, Add, Modify
	`fimain`	Grants access to the Field Interview Search screen.	Access
	`frfimain`	Grants access to the Fire Field Interview Search screen.	Access
	`frmain`	Grants access to the Fire Incident Search screen.	Access
	`inmisc`	Grants access to the Miscellaneous Involvement Search screen.	Access
	`jlarrest`	Grants access to the Arrest Search screen.	Access
	`jmarrest`	Grants access to the Classic Arrest Search screen.	Access
	`lpmain`	Grants access to the License and Permit Search screen.	Access
	`lwcase`	Grants access to the Case Management Search screen.	Access
	`mdcadmagncymsg`	Grants access to the **Edit Agency/Dept. Message** option on the Tools menu.	Access
	`mdcadmagncyprefs`	Grants access to the Create Default Settings screen, but forces the **Agency** option in the **Set defaults for** area to be pre-selected with the agency of the user. The **Set defaults for** area is read-only.	Access

Module	System Privilege	Description	Privilege
	`mdcadmoptions`	Grants the ability to access the Options dialog box to modify search, sounds, CAD, color, Mapping, and Messaging options.	Access
	`mdcadmtoolbars`	Allows the user to customize the primary toolbar and shortcut keys.	Access
	`nmcrtnot`	Grants access to the Critical Notice Search screen	Access
	`nmmain`	Grants the ability to add or edit Name records from Mobile.	Add, Modify
	`pnactiv`	Grants access to the Pawn Activity Search screen.	Access
	`pnmain`	Grants access to the Pawned Property Search screen.	Access
	`prmain`	Grants the ability to add or edit Property records from Mobile.	Add, Modify
	`twmain`	Grants access to the Traffic Warning Search screen.	Access
	`vhmain`	Grants the ability to ability to add or edit Vehicle records from Mobile.	Add, Modify
	`vimain`	Grants access to the Impound Search screen.	Access
	`wamain`	Grants access to the Wanted Person Search screen.	Access

Giving a user administrative access

The following table lists the administrative privileges that can be given to a user and the required modules. Privileges can be set at a User, Group, or Agency level.

Module	System Privilege	Description	Privilege
Approvals (`mdcmdlworkflow`)	`mdcadmworkflow`	Enables the **Supervisor** folder for the Workflow Management feature.	Access
Automated Field Reporting	`geninc`	Grants the ability to save form data. Required for all users of General Use or State forms. This setting applies to the PDF forms only.	Add, Modify

Module	System Privilege	Description	Privilege
AVL & Mapping (`mdcmdlmapping`)	`mdcadmonetouch`	Grants the ability to change the **One-Touch Status** buttons from the default on the Mobile Mapping screen. This also disables the **Restore Defaults** button.	Access
Driver License Scanning (`mdcmdldlscan`)	`mdcadmdlscan`	Grants the ability to turn on and off the Auto-search on scan option in Mobile.	Access
RMS Queries (`mdcmdllocquery`)	`mdcadmtemplates`	Enables the **Templates** button on the Create New Supplemental Narrative and Append Supplemental Narrative windows.	Access
Voiceless CAD (`mdcmdlcad`)	`mdcadmgetinci`	Grants the ability to create incidents on demand using the **Incident #** button on the CAD and Radio Log History screens.	Access
	`mdccadunitstatus`	Grants access to the Unit Status screen.	Access
	`mdcadmassignunit`	Grants the ability to assign self to a unit during the login process.	Access
(none)	`mdcadmalerts`	Grants the ability to modify, dismiss, and set expiration times for ATL, BOLO, and Emergency alerts sent by other users. For general users to send ATL, BOLO, and Emergency alerts, no special privileges are required. This privilege affects any alert in the Message Center, on the Mobile map, or on the CAD map.	Access, Add, Modify
	`mdcadmconnect`	Grants access to the Connection Settings dialog box. From this dialog box, users can change their Client ID, Vehicle ID, and Unit. For more information, see "Changing the assigned client ID, vehicle ID, or unit" on page 65.	Access

Changing the Mobile server and port

Mobile settings can be modified from the Mobile Login screen. By default, if Mobile is opened at the same time as Flex, then Mobile obtains the necessary settings from Flex. The settings are saved for subsequent sessions, and Mobile can be opened without opening Flex. However, the server and port settings for Mobile can be added manually or changed, if desired.

To change the Mobile server and port:

1. From the Mobile Login screen, click the **Detail** link.

   The **Server** and **Port** fields appear.

2. Complete the following fields:

   – **Server**: Enter the name of your server.

   – **Port**: Enter the Mobile port number. The default is `22630`.

3. If necessary, to modify the Spillman port, press Ctrl+Shift+A.

The **Spillman Port** field appears.

4. Enter the desired port number. The default is `4080`.

5. When finished, log in to Mobile.

Creating Mobile shortcuts that access different servers

Multiple shortcuts for Mobile can be created, and each shortcut can be configured to access a different server. For example, if the Training database and the Live database are on separate servers, then create two shortcuts on the desktop—one that accesses the Training database and one that accesses the Live database.

To create multiple shortcuts that access different servers:

1. Create a shortcut to Mobile on the desktop.

2. Right-click the shortcut to open a menu of options.

3. Click **Properties**.

   The Mobile Properties dialog box opens.

4. Click the **Shortcut** tab.
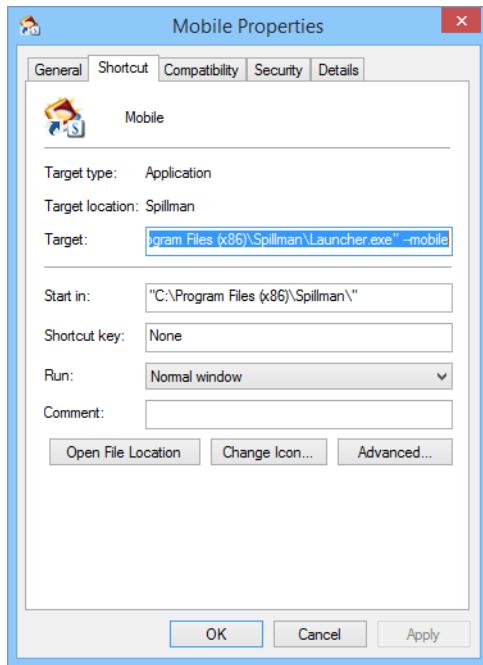
5. In the **Target** field, place the cursor after the name of the executable file, and then add a space. If the file name is followed by a quotation mark, then place the cursor after the quotation mark.

6. Enter the server's IP address and port, using the following format:

   /host *IP-address* /port *port-number*

   where *IP-address* is your IP address and *port-number* is your Mobile port number.

7. Click **OK**.

8. Rename the shortcut to indicate which server it accesses.

9. Repeat steps 1–8 for each server that needs a shortcut.

10. The next time Mobile needs to be started, double-click the shortcut for the desired server and log in as usual.

Updating the Agency or Department Message

In addition to the Message of the Day, an agency- or department-specific message can be displayed on the Mobile Today screen. To update the message, either Super User (SU) privileges or the `mdcadmagncymsg` privilege is required. For more information on setting the `mdcadmagncymsg` privilege, see "Setting up system privileges for Mobile" on page 44.
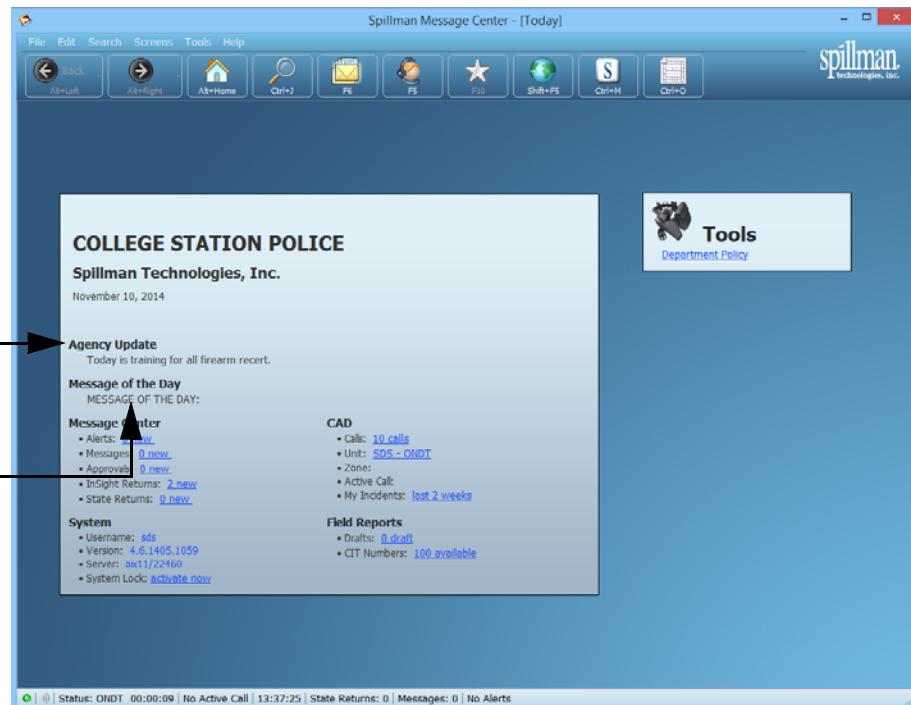
To update the agency or department message:

1. From the menu bar, select **Tools** > **Edit Agency/Dept. Message**.

The Edit Agency/Dept. Message dialog box opens.
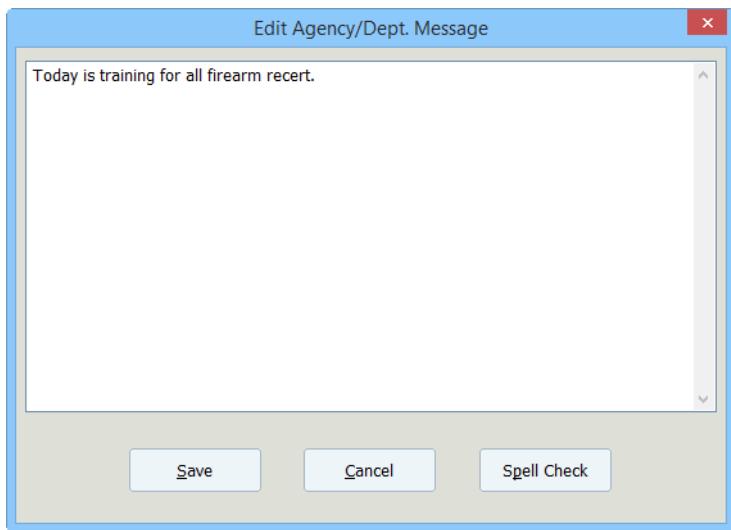
2. Enter the message to display. The message is limited to 800 characters in length.

3. Click **Save**.

Your message is displayed on the Mobile Today screen.

> **NOTE**
>
> If a Message of the Day has been set, it is displayed below the **Agency Update** or **Department Update** area.

Adding your agency logo to the Today screen

The Mobile Today screen can display your agency or department logo.

To add an agency or department logo to the Mobile Today screen:

1. Create a PNG (`.png`) or GIF (`.gif`) file of your agency's logo.

> **NOTE**
>
> For best results, the background of the logo should be transparent. It is not recommended to use JPG (`.jpg`) files, as they cannot have a transparent background.

2. To name the file, do one of the following:

   – To set the logo for all users, use the following format:

`logo.`*`extension`*

where *extension* is the file extension for the type of image file.

– To set a logo for each agency, use the following format:

`agencycode.extension`

where *agencycode* is the code for your agency (`apagncy`) and *extension* is the file extension for the type of image file. For example, if your agency code is SPD, then name the file **`SPD.png`**.

3. Place the file in one of the following directories:

– For all users, place the file in

`\uclient\all\html\images`

– For each agency, place the file in

`\uclient\`*`agencyname`*`\html\images`

where *agencyname* is the name of the folder for the agency to which the logo belongs.

The Mobile Today screen displays your agency or department logo.

Creating default settings for a group, agency, or all users

The following settings can be set for Mobile from your computer, and then applied to other users as default settings:

▪ Toolbar and keyboard

▪ Options dialog box

▪ Messaging groups

The settings can be set for all users, by agency, or by group. To use this feature, either SU privileges or the `mdcadmagncyprefs` privilege is required.

> **NOTE**
>
> If the settings are being applied using the `mdcadmagncyprefs` privilege, then the settings are applied only to the agency of the person updating the settings.

To save your settings as the default settings for a group, agency, or all users:

1. From the menu bar, select **Tools** > **Create Default Settings**.

The Create Default Settings dialog box opens.
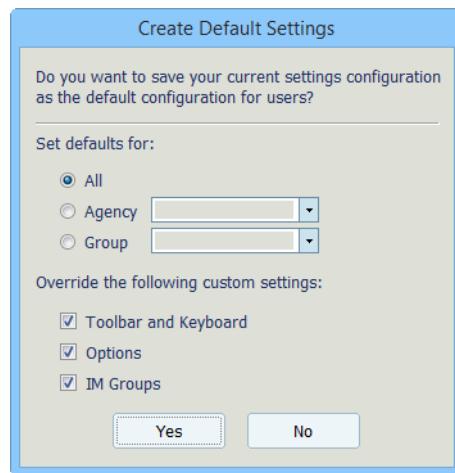
2. In the **Set defaults for** area, do one of the following:

   – To apply the settings to all users, select **All**.

   – To apply the settings to a specific agency, select **Agency**, and then select the agency from the drop-down list.

   – To apply the settings to a specific group, select **Group**, and then select the group from the drop-down list.

3. To override custom settings that users might have set on their computers, in the **Override the following custom settings** area, do any of the following:

   – To override custom toolbar and keyboard settings set in the Customize dialog box, select the **Toolbar and Keyboard** check box.

   – To override custom settings in the Options dialog box, select the **Options** check box.

   – To override custom IM groups, select the **IM Groups** check box.

4. Click **Yes**.

   The default and custom settings are removed according to the options selected and the new default settings are applied.

Working with the Mobile color themes

The color theme is based on the value in the **Unit Type** field on the Units table (`cdunit`). For example, Fire and EMS users view a theme called Fire Mobile. Fire Mobile includes a red-based color palette, a Fire Mobile logo, and Fire-specific verbiage.

Fire Mobile logo

Tools area with Fire theme
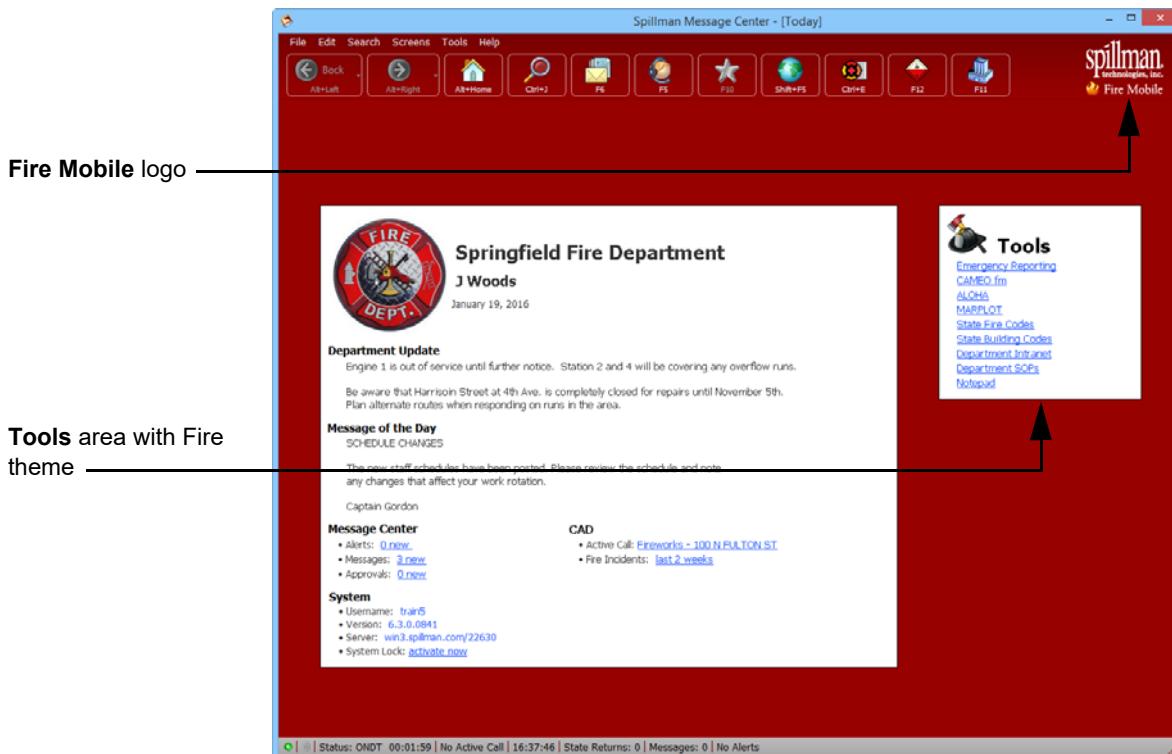
However, the color theme can be changed at anytime using the **Colors** tab in the Options dialog box.

To change the color theme:

1. From the menu bar, select **File** > **Options**.

   The Options dialog box opens.

2. Click the **Colors** tab.
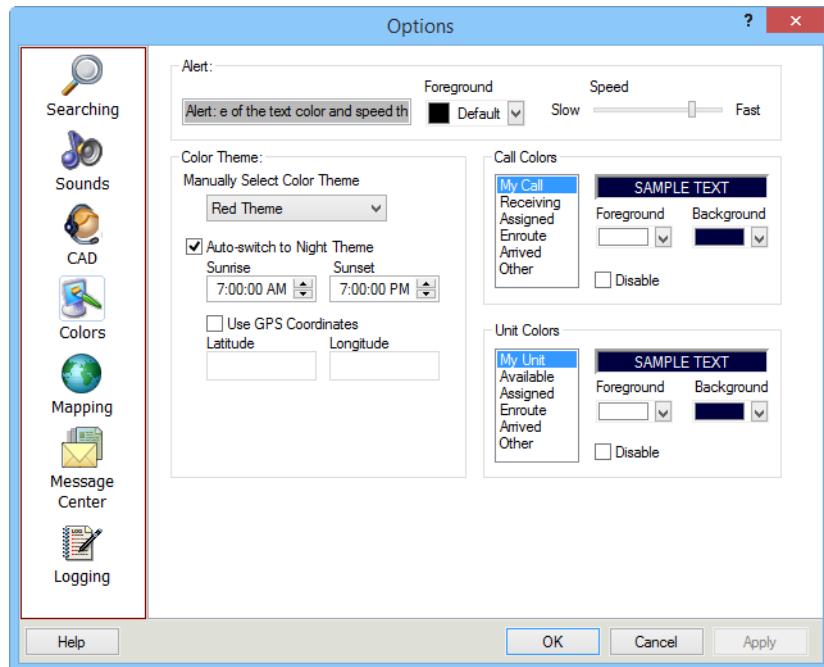
3. In the **Color Theme** area, in the **Manually Select Color Theme** field, select a color theme from the drop-down list.

> **NOTE**
>
> If the **Unit Type** field on the Units table (`cdunit`) is left blank, then by default, the color is set to `Blue Theme`.

4. To preview your changes, click **Apply**.

5. Click **OK** to accept changes, or click **Cancel** to keep the options unchanged.

Customizing sounds for Mobile

Sound notifications in Mobile can be customized and additional Waveform Audio File Format (`.wav`) sound files can be added to a computer.

Sound notifications are associated with the following events:

- Local Query Received
- State Query Received
- State Voice Response
- My Call Updated
- Other Calls Updated
- New Mail Message

- New Alert
- Instant Message Sent
- Instant Message Received
- Urgent Instant Message Sent
- Urgent Instant Message Received
- Approval Recieved

To customize sounds:

1. Navigate to the following directory:

   `$MOBILEDIR\uclient\`*`folder`*`\sounds`

   where *folder* is the desired location for the sounds to be applied. Sounds can be applied to all users in an agency, groups of users, or individual users. For example, to apply the sounds to a specific agency, navigate to

   `$MOBILEDIR\uclient\`*`agencyname`*`\sounds`

   where *agencyname* is the name of the folder for the agency.

2. In the **Sounds** folder, add the WAV sound files.

   The sounds are available to users the next time they log in to Mobile.

3. Log out of the software, and then log back in.

4. To change the sound notification for an event, select **File** > **Options** (Alt, F, O).

   The Options dialog box opens.

5. Automatically opening single search results

6. Click the **Sounds** tab.
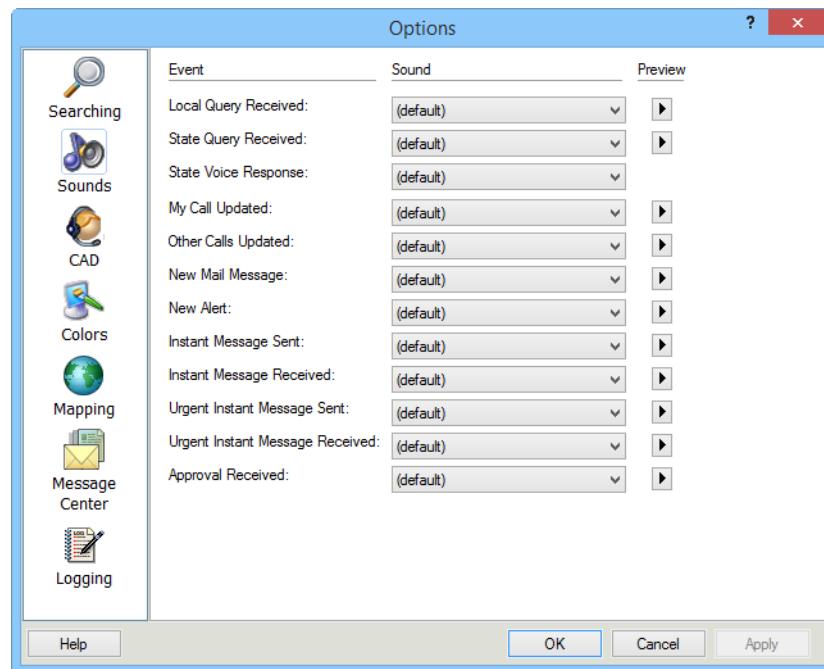
7. In the **Sound** field for the desired event, select a sound from the drop-down list, or select **None** to play no sound. To preview the sound, click the **Preview** button.

8. Repeat steps 4–6 for all desired event sounds to change.

9. Click **OK** to save your changes.

10. If necessary, apply the settings to other users. For more information, see "Creating default settings for a group, agency, or all users" on page 55.

Setting local returns to open in Flex

Local returns for Name and Vehicle records can be opened in Flex when the software has a connection to Mobile. The following settings in the Administration Manager (`adminutil`) dictate whether users are able to open local returns in Flex.

The following setting is found in the **Module.MobileCallSettings** folder in the Administration Manager.

Setting	Description	Value
ShowOpenButtonForLocalRecords		True/False
	Determines whether the **Open** button is available to open local returns in Flex. • Set to **True** to make the **Open** button available. • Set to **False** to make the Open button unavailable. The default value is False.	

The following setting is found in the **Module.CAD** folder in the Administration Manager.

Setting	Description	Value
MessageCenterOpenSingleSearchResult		True/False
	Determines whether a query with a single search result opens automatically in Flex. • Set to **True** to open single results automatically. • Set to **False** to prevent single results from opening automatically. The default value is False.	

Setting Up Application Parameters

The following table lists the application parameters that affect Mobile. In the Application Parameters table (`apparam`), set the parameters according to the desired behavior. For more information on setting up application parameters, see the *Application Setup and Maintenance Manual*.

> **NOTE**
>
> In addition to setting the application parameters described in this manual, the `logmodes` and `lognames` system parameters should also be set in the System Parameters table (`syparam`).
>
> If your agency did not set the `logmodes` and `lognames` system parameters when the RMS module was set up, then see the *Application Setup and Maintenance Manual* for further instructions.

Parameter	Description	Value
`autokick`	`Mandatory Logoff`	Numeric
	Determines how long a user can be logged in to Mobile before being logged off. In the first line of the text editor, enter the maximum number, in minutes, for a user to remain logged in to the system. In the second line, enter the number of minutes to be remaining when the user is prompted with a warning before being logged off. To set multiple warnings, enter the number of minutes separated by a comma. For example, enter **5,10,15** to warn a user when 15, 10, and then five minutes remain until they are logged off.	
`cdoffro`	`CAD Disable Reordering Officers for Agencies`	Alphanumeric/All/(blank)
	Determines which agencies do not reorder the responsible and secondary officers when the Update Officer (UO) command is used to assign an officer to a unit, and the officer logs in to Mobile. • Enter the name of each agency, separated by a comma, to disable reordering officers for specific agencies. • Set to **All** to disable reordering officers for all agencies. • Leave the value blank to continue reordering officers for all agencies. By default, the value is blank.	
`ctautono`	`Citation/Traffic Automatic Num`	Yes/No
	Determines whether the Mobile Citation or Warning forms automatically populate with new form numbers when they are opened. • Set the value to **Yes** to automatically populate form numbers. • Set the value to **No** to require officers to enter a form number. **NOTE**: This parameter applies only to the Mobile PDF forms. It does not apply to the State eCitation or State Crash forms. For information on how to set up the State eCitation and State Crash forms, see the *Mobile State eCitation and State Crash Forms Manual*.	

Parameter	Description	Value
`lmtinvl`	`Mobile Involvement Limit`	Numeric
	Determines the limited number of involvements returned with a Mobile query. Enter the maximum number of involvements to be returned with each query. By default, the value is `50`.	
`lockform`	`Lock Forms by Workflow Status`	Alphabetic
	Locks forms from future changes according to their workflow status. Enter any workflow statuses, separated by a comma, to lock a form according to the workflow status entered. For example, enter **`COMPLT,LOCK,REMIT`**. For more information, see "Locking Mobile forms from future changes" on page 123.	
`msgrxcmd`	`Msg Cntr Command Line Control`	`True/False`
	Determines whether the Message Center can be controlled at the command line. • Set to **`True`** to use CAD commands to control the Message Center. For a list of commands, see the *Mobile User Manual*. • Set to **`False`** to not use CAD commands to control the Message Center.	
`narrtime`	`Show Time Stamp Mobile Narratives`	`Yes/No`
	Determines whether a time and date stamp is added to narratives. • Set to **`Yes`** to automatically stamp narratives with a time and date. • Set to **`No`** to prevent the software from stamping the narrative with a time and date.	
`prschfst`	`Require Property Search to Add`	`True/False`
	Determines whether a search is required to add a Property record. • Set to **`Yes`** to require a search before adding a Property record. • Set to **`No`** to allow a Property record to be added without first performing a search.	
`sepstret`	`State Rtrn from Ccmts`	`True/False`
	Determines whether state returns attached to a call are viewed in the call comments, or if they are separated and viewed in the **State Returns** tab or using the **StateRtn** button. • Set to **`True`** to enable the **State Returns** tab and **StateRtn** button. The **State Returns** tab is located in the CAD Call Information screen in Mobile Voiceless CAD and the Call Comments screen in CAD. The **StateRtn** button is located in the CAD Call Taker's screen. For more information, see the *Mobile User Manual* and the *CAD User Manual*. • Set to **`False`** to attach state returns to call comments and hide the **State Returns** tab and **StateRtn** button. By default, the value is `False`. For more information, see the StateLink manual.	

Setting the Client ID and Vehicle ID

Depending on the settings and requirements for your agency, the **Vehicle ID** and **Client ID** fields in the Mobile Login screen might need to be completed to use Mobile.

About client IDs Mobile can be used in either a static or dynamic IP network. To use Mobile in a dynamic IP network, a unique identifier called a client ID must be assigned to each computer that runs Mobile. To prevent two users from logging on with the same client ID, in the `options.xml` file, set the `AllowDuplicateClientIDs` setting to **false**. For more information, see "Defining XML tags for the Mobile server" on page 27.

> **NOTE**
>
> Assigning a client ID is optional if your agency has a static IP network. If a client ID is not assigned, then the Mobile server identifies the computer by its IP address.

About vehicle IDs Certain CJIS security requirements dictate that agencies must use the IP address for the Mobile client for identification. If your agency is using software to alter the client IP address as seen by the server, then the IP address for the client is not the same as the IP address for the modem reporting AVL information. If the client IP address is not the same as the modem IP address, then the **Vehicle ID** field is used to communicate with the AVL server.

Assigning a client ID or vehicle ID

In some cases, the client ID and vehicle ID are assigned when the software is installed. However, the client ID and vehicle ID can be assigned when logging in to Mobile, or they can be changed as needed. A client ID or vehicle ID is a unique combination of letters, numbers, or both. The client ID and vehicle ID must be nine or fewer characters.

To assign a client ID or vehicle ID after installing Mobile:

1. Start Mobile.

The Mobile Login screen opens.

2. Do any of the following:

   – In the **Client ID** field, enter the desired client ID.

   – In the **Vehicle ID** field, enter the desired vehicle ID.

3. Click **Login** to begin the Mobile session.

Changing the assigned client ID, vehicle ID, or unit

If the required privileges have been granted, then the client ID, vehicle ID, and unit can be changed from the Connection Settings dialog box. For more information, see "Setting up system privileges for Mobile" on page 44.

To view the current client ID and vehicle ID, from the menu bar, select **Help > About Spillman Mobile**.

To change the assigned client ID or vehicle ID:

1. From the menu bar, select **Tools > Connection Settings**.

   The Connection Settings dialog box opens.

2. Modify any of the following fields as needed:

   – **Client ID**: Enter a new client ID

   – **Vehicle ID**: Enter a new vehicle ID.

   – **Unit**: Enter a new unit ID.

3. Click **OK**.

   The Connection Settings dialog box closes and the new settings are applied to the Mobile client.

Restricting access to the Client ID and Vehicle ID fields

The **Client ID** and **Vehicle ID** fields can be hidden from the Mobile Login screen by modifying the registry on the computers for the users who should not access those fields.

> **TIP**
>
> To save time, Windows administration techniques can be used to adjust these settings for multiple users simultaneously.

To restrict access to the **Client ID** and **Vehicle ID** fields:

1. Open your Registry Editor.

2. Locate the `Mobile Settings` subkey in the `HKEY LOCAL MACHINE` root key by selecting the following:

   HKEY_LOCAL_MACHINE > **Software** > **Wow6432Node** > **Spillman** > **Mobile** > **Settings**

3. Right-click in the **Values** area and select **New** > **DWORD (32-bit) Value**.

4. Do one of the following:

   – To disable access to the **Client ID** field, enter **`ClientIDEnabled`**, and then press Enter.

   – To disable access to the **Vehicle ID** field, enter **`VehicleIDEnabled`**, and then press Enter.

   By default, in the **Data** column, the value is set to `0`, which means the respective field is disabled and the user cannot modify the field in the Login dialog box. If the value is anything other than `0`, or if the setting does not exist in the registry, then the respective field is enabled and can be accessed.

> **NOTE**
>
> Users are able to see their client ID and vehicle ID in the **Client ID** and **Vehicle ID** fields. However, the ability to make changes to the fields is disabled.

If the **Client ID** field is disabled, then the `EClientID` value in the `HKEY LOCAL MACHINE` root key is used. This forces the client ID to

be specific to the computer that the user is accessing during the session.

> **NOTE**
>
> For Windows Vista and Windows 7, normal use of Mobile does not allow users to edit values in the `HKEY LOCAL MACHINE` root key. If access to the client ID is restricted, then Mobile must initially be run under an administrator login. At this time, the software encodes the client ID and transfers the information to `EClientID` for future use.

Setting Up CAMEO Chemicals

Opening the Hazmat Search screen launches CAMEO (Computer-Aided Management of Emergency Operations) Chemicals. If your users have an active Internet connection, no action is required for setup. If no Internet connection is available, then to use CAMEO Chemicals, the software must be installed on the computer.

To download CAMEO Chemicals:

1. In a web browser, navigate to the following URL:

   http://www.epa.gov/cameo

   The EPA website opens to the CAMEO page.

Download CAMEO Chemicals link ⟶
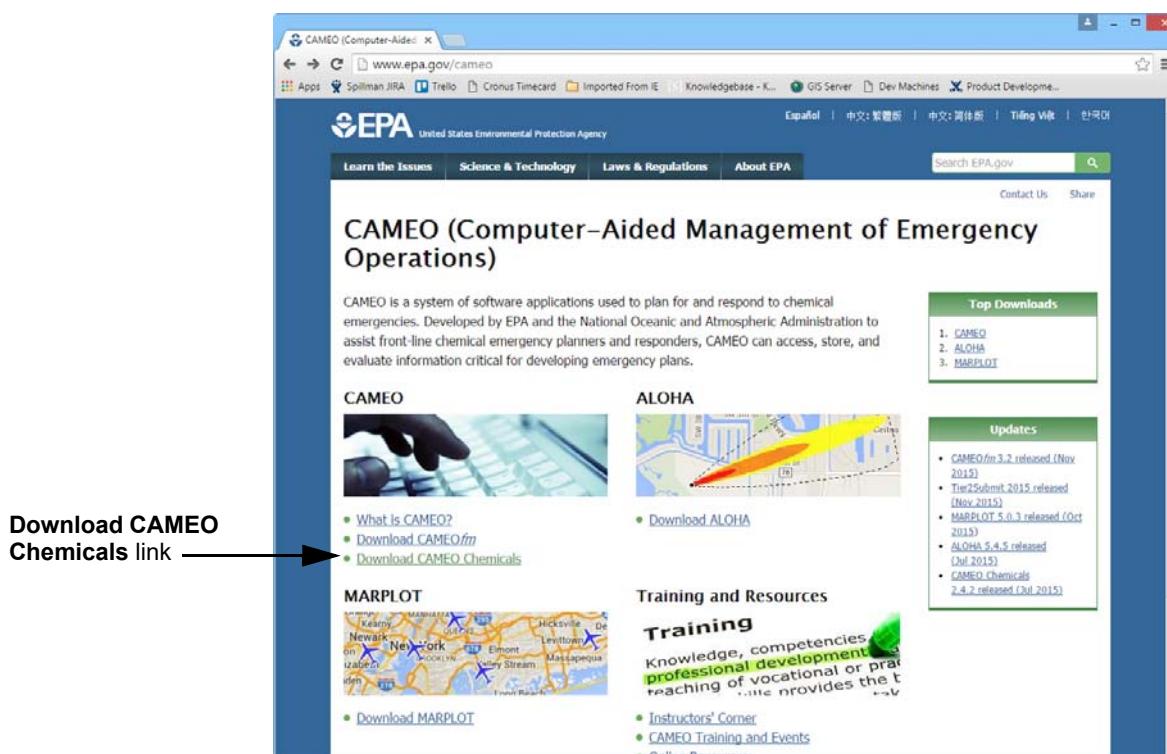
2. Click the **Download CAMEO Chemicals** link.

   The site navigates to the area where the download link is located.

3. Click the **Download CAMEO Chemicals for Windows** link.

4. Follow the installation steps.

   CAMEO Chemicals is installed and available for offline use.

Chapter 2

Setting Up Mobile Modules

Jump to topic:

Introduction

This chapter contains administrative information specific to the following modules:

- Mobile Driver License Scanning. See "Setting Up the Mobile Driver License Scanning Module" on page 73

- Mobile Voiceless CAD. See "Setting Up the Voiceless CAD Module" on page 77.

- Mobile Mapping. See "Setting Up the Mapping Module" on page 92.

- Automated Field Reporting. See "Setting Up the Automated Field Reporting Module" on page 112

In addition, information about how to set up and use the Translation Administration Tool to translate database codes to state codes is also described. For more information, see "Using the Translation Administration Tool" on page 129.

To use the Field Manager to modify files in the Add Record or Edit Record screens for Names, Vehicles, and Property, see "Using the Field Manager" on page 145.

For information on additional modules that work with Mobile, such as the Automatic Vehicle Location module (AVL), see the manuals for those modules.

> **NOTE**
>
> For the Mobile RMS Queries and Mobile Premises Information modules, only the general setup tasks outlined in "Installation and Setup" on page 13 must be performed.

Setting up units for Mobile

Each unit that uses Mobile must be specified in the Units table (`cdunit`). This is required for units to work with modules such as Voiceless CAD or Mobile Mapping, in addition to the setup tasks and privileges described in the section for each module.

To set up a unit for Mobile:

1. At the command line, enter `cdunit`.

The Units table opens.
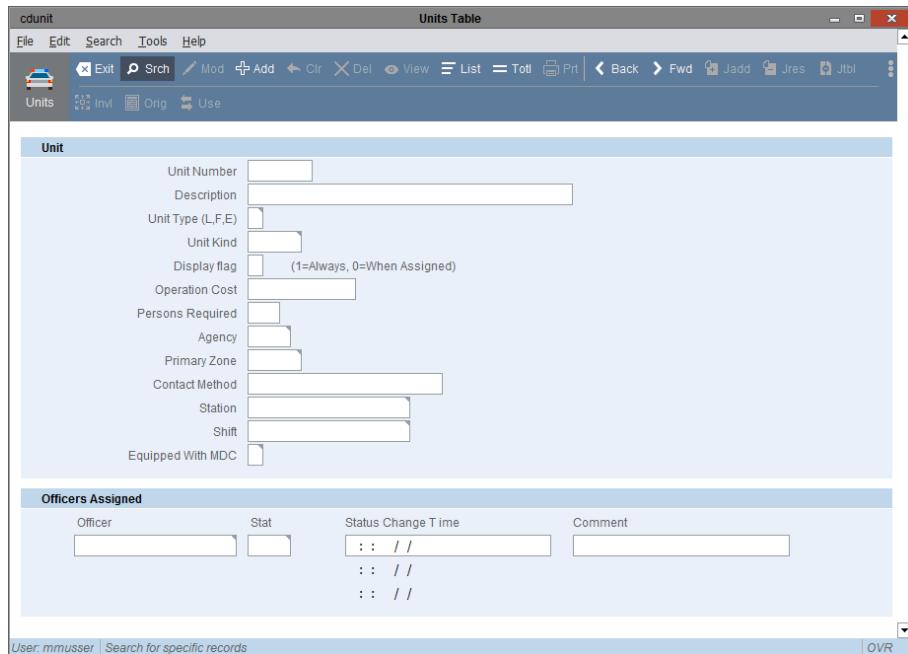
2. Click **Srch**, and then search for the desired unit.

3. With the record displayed, click **Mod**.

4. In the **Equipped With MDC** field, enter `y`.

5. Click **Accept** (Alt+A).

    The record is updated with your changes.

6. Repeat steps 2–6 for each unit that uses Mobile.

7. Click **Exit** to close the Units table.

Creating a status sequence for a unit

The status sequences that were created as part of setting up CAD in Flex can also be used for Mobile. However, additional Responding Unit Status Order table (`cdstatse`) records can be created to set up different status sequences, if desired.

For example, for unit kind `AMB` (ambulance), a `cdstatse` record with a sequence similar to the following might be created.

Status field value		Becomes field value	
Call status	Meaning	Unit status	Meaning
RCVD	Received the call	RCVD	Received the call
ENRT	En route to the scene	ENRT	En route to the scene
ARRVD	Arrived at the scene	ARRVD	Arrived at the scene
ENRTH	En route to the hospital	ENRTH	En route to the hospital
HOSP	At the hospital	HOSP	At the hospital
RETRN	Returned to the station	RETRN	Returned to the station
CMPLT	Completed the call	ONDT	On duty

NOTE

Every value entered in the **Status** or **Becomes** fields must be defined by a code in the Unit Status Ten-Codes (`tb10code`) table. For more information on setting up a status sequence, see the *Application Setup and Maintenance Manual*. For more information on the `tb10code` table, see the *Code Table Setup and Maintenance Manual*.

Setting Up the Mobile Driver License Scanning Module

If your agency uses the Mobile Driver License Scanning module, then officers have the ability to swipe or scan a driver license as an alternative to manually entering the data to send to state and local queries.

For a list of scanning devices compatible with Mobile, see the Technical Product Description (TPD) for the Driver License Scanning module. For a copy of the TPD, contact your Spillman Client Services representative or Spillman Technical Services.

> **NOTE**
>
> Some state bar codes encrypt certain data elements. If your state uses encrypted barcodes, then the encryption key can be requested from the state. When permission is granted in writing, contact Spillman Technical Services for assistance in enabling the decryption system.

Before performing the tasks in this section, complete the general setup tasks outlined in "Installation and Setup" on page 13.

To set up the Mobile Driver License Scanning module, complete the following:

- "Enabling the module" on page 73
- "Setting additional driver license scanning options" on page 75

Enabling the module

To use the Driver License Scanning module, the module must be enabled and the communication settings must be set up for the device.

To enable the module:

1. From the menu bar, select **File** > **DL Scanning** > **Enable**.

The Enable DL Scanning dialog box opens.
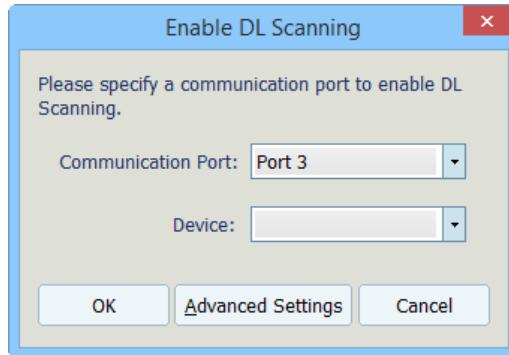
2. Complete the following fields:

 – **Communication Port**: Select the port to use to communicate with the device from the drop-down list.

 – **Device**: Select the type of device from the drop-down list.

3. To set advanced communication port settings, click **Advanced Settings.**

The DLScan Advanced Settings dialog box opens.
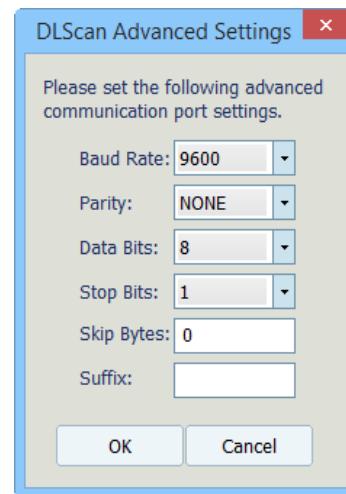
4. Complete the following fields as necessary:

 – **Baud Rate**   – **Stop Bits**

 – **Parity**   – **Skip Bytes**

 – **Data Bits**   – **Suffix**

For information on the optimal settings for your device, consult the user documentation for the device.

5. Click **OK** to close the dialog box and apply your settings.

6. Repeat steps 1–5 for each user that will use the module.

Setting additional driver license scanning options

In the Options dialog box, additional optional settings for the Driver License Scanning module are available.

To set additional driver license scanning options:

1. From the menu bar, select **File** > **Options**.

   The Options dialog box opens. By default, the **Searching** tab is selected.

Driver License Scanning area
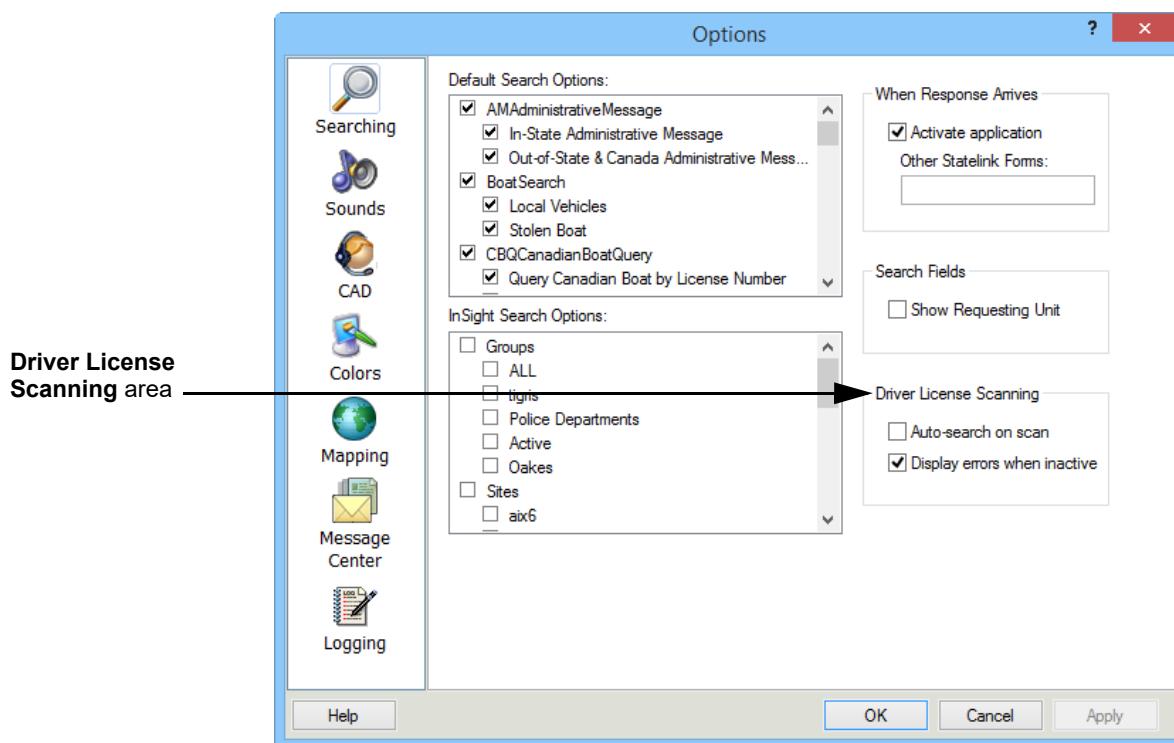
2. In the **Driver License Scanning** area, do any of the following:

   – To automatically perform a search when a driver license is swiped or scanned, select the **Auto-search on scan** check box.

If the check box is cleared, then the Name Search screen opens and the information is populated, but the officer must click the **Search** button to perform a query.

– To display scanning errors when Mobile is not the active application, select the **Display errors when inactive** check box.

If the check box is cleared, then scanning errors are not displayed while Mobile is not the active application.

NOTE

Magnetic stripes and bar codes can deteriorate over time. If this happens, then errors can occur. The software will populate as much of the data as it can read to the Name Search screen. Depending on your settings, an error message is displayed.

---

3. Click **OK** to apply your changes and close the Options dialog box.

4. If necessary, apply the settings to other users. For more information, see .

Setting Up the Voiceless CAD Module

This section contains setup and maintenance information for the Mobile Voiceless CAD module. Before performing the tasks in this section, complete the general setup tasks outlined in "Installation and Setup" on page 13 and "Setting up units for Mobile" on page 70.

To set up the Voiceless CAD module, complete the following:

- "Defining the ten-codes used in Mobile" on page 77
- "Defining the disposition codes used in Mobile" on page 78
- "Setting up MDC units" on page 79
- "Setting up the One-Touch Status buttons" on page 80
- "Configuring the CAD filter" on page 84
- "Adding additional Mobile alert codes" on page 87
- "Managing the CAD Web Aggregator" on page 88
- "Setting CAD colors" on page 89
- "Managing CAD settings in the Administration Manager" on page 90

Defining the ten-codes used in Mobile

By default, all the ten-codes in the Unit Status Ten-Codes table (`tb10code`) are used in Mobile. However, some ten-codes in `tb10code` might not apply to officers in the field.

To define which ten-codes are used in Mobile:

1. At the command line, enter **`tb10code`**.

The Unit Status Ten-Codes table opens.
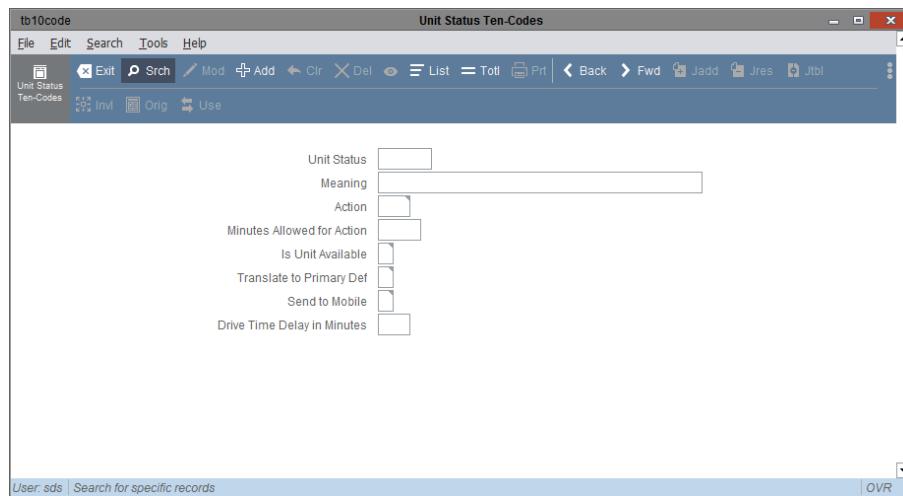
2. Search for the ten-code to modify.

3. With the desired record open, click **Mod**.

4. In the **Send to Mobile** field, do one of the following:

   – To send the code to Mobile, enter **Y**.

   – To not send the code to Mobile, enter **N**.

5. Click **Accept** (Alt+A).

6. Repeat steps 2–5 for each ten-code to be modified.

7. Click **Exit** to close Unit Status Ten-Codes table.

> **NOTE**
>
> To highlight a status with a specific background color in Voiceless CAD, the **Send to Mobile** field must contain a value of **Y** and the action code entered in the **Action** field must contain the value that is associated with the desired color in your color settings in the Options dialog box. For more information, see "Setting CAD colors" on page 89.

Defining the disposition codes used in Mobile

When the responsible officer closes a call, the Complete Call dialog box opens. In the **Disposition** field, the drop-down list contains all the dispositions from which the officer can choose to close the call.

By default, all disposition codes in the Law Incident Disposition Codes table (`lwtbdisp`) are used in Mobile. However, some disposition codes in this table might not apply to officers in the field.

To define which disposition codes are used in Mobile:

1. At the command line, enter **`lwtbdisp`**.

   The Law Incident Disposition Codes table opens.

2. Search for the disposition code to modify.

3. With the desired record open, click **Mod**.

4. In the **Send to Mobile** field, do one of the following:

   – To send the code to Mobile, enter **`Y`**.

   – To not send the code to Mobile, enter **`N`**.

5. Click **Accept** (Alt+A).

6. Repeat steps 2–5 for each disposition code to be modified.

7. Click **Exit** to close Law Incident Disposition Codes table.

Setting up MDC units

Voiceless CAD can be used with any unit that is set up in the Units table (`cdunit`) to use Mobile, as long as the user has been given the appropriate privileges. However, if desired, your agency can set up a specific unit kind to identify units that have Mobile, also known as Mobile Data Computer (MDC) units.

To set up MDC units, complete the following tasks:

▪ In the Public Safety Vehicle codes table (`tbvehknd`), add a record for each type of MDC unit. For example, `MDS Mobile Data Supervisor`, or `MDP Mobile Data Patrol`.

▪ Add each unit to `cdunit`. In the **Unit Kind** field, enter the code for each unit, such as **`MDS`** or **`MDP`**, to remind users that the unit follows the status sequence for MDC units.

▪ Create a status sequence for each type of MDC unit. See "Creating a status sequence for MDC units" on page 80.

▪ Activate each unit by creating a Radio Log record. To create a Radio Log record, place each unit off duty. For more information, see the *Application Setup and Maintenance Manual*.

The new units are ready to use. For more information on the `tbvehknd` and `cdunit` code tables, see the *Code Table Setup and Maintenance Manual*.

Creating a status sequence for MDC units

To create a status sequence specifically for MDC units, create a record in the Responding Units Status Order table (`cdstatse`) for each MDC unit kind. The following table describes the recommended status sequence for an MDC unit.

Status field value	Becomes field value
RCVD	RCVD
ASSGN	ASSGN
ENRT	ENRT
ARRVD	ARRVD
CMPLT	ONDT

When a dispatcher uses the recommended status sequence to dispatch a call to an MDC unit, the status of the call becomes `ASSGN`. When an officer in that unit changes the unit status from `ASSGN` to `ENRT`, the status of the call changes to `ENRT`, and the dispatcher knows that the unit received the call.

Setting up the One-Touch Status buttons

If your agency uses the One-Touch Status buttons, then they can be displayed on the left side of the Mobile map.

The One-Touch Status buttons are defined by the most relevant record in the Responding Units Status Order table (`cdstatse`), and can be set according to agency or type of unit. The button names are populated from the first eleven statuses found in the `cdstatse` record. For more information, see "Understanding which Responding Units Status Order record is used" on page 84.

To set up the One-Touch Status buttons:

1. If desired, in the Responding Units Status Order table, set up status sequences for the One-Touch Status buttons. For more information, see "Creating a status sequence for One-Touch Status buttons" on page 82.

2. From the menu bar, select **File** > **Options**.

The Options dialog box opens.
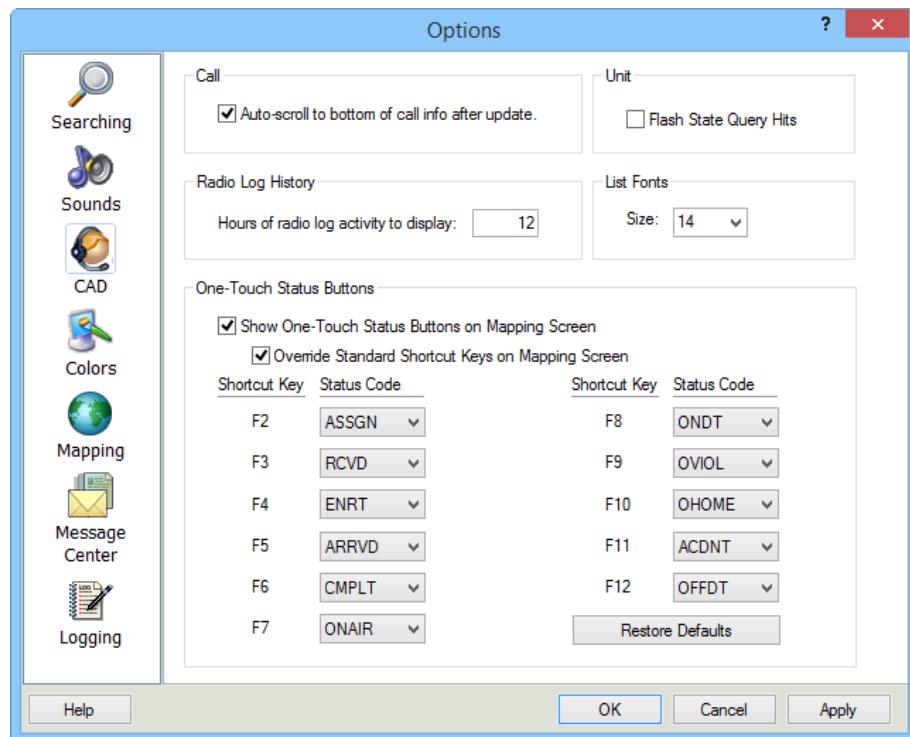
3. Click the **CAD** tab.

4. In the **One-Touch Status Buttons** area, do any of the following:

   – Select or clear the **Show One-Touch Status Buttons on Mapping Screen** check box to show or hide the One-Touch Status buttons from the map.

   – Select or clear the **Override Standard Shortcut Keys on Mapping Screen** check box to override the default shortcut behavior for the keyboard shortcut keys, or to use the default shortcut key behavior. If the check box is selected, then the appropriate shortcut key for the status is displayed on the button when the buttons are displayed on the map.

   – To assign a specific status to a shortcut key, in the **Status Code** column, select the desired status from the drop-down list located next to the shortcut key name. To reset the buttons to the default values, click **Restore Defaults**.

5. Click **OK** to apply your changes and close the Options dialog box.

6. If necessary, apply the settings to other users. For more information, see "Creating default settings for a group, agency, or all users" on page 55.

Creating a status sequence for One-Touch Status buttons

If no status sequences are specified for One-Touch Status buttons, then existing Responding Unit Status Order records are used, as described in "Understanding which Responding Units Status Order record is used" on page 84. For more information on creating a status sequence, see "Creating a status sequence for a unit" on page 71.

To create a status sequence for One-Touch Status buttons:

1. At the command line, enter **cdstatse**.

   The Responding Units Status Order table opens.
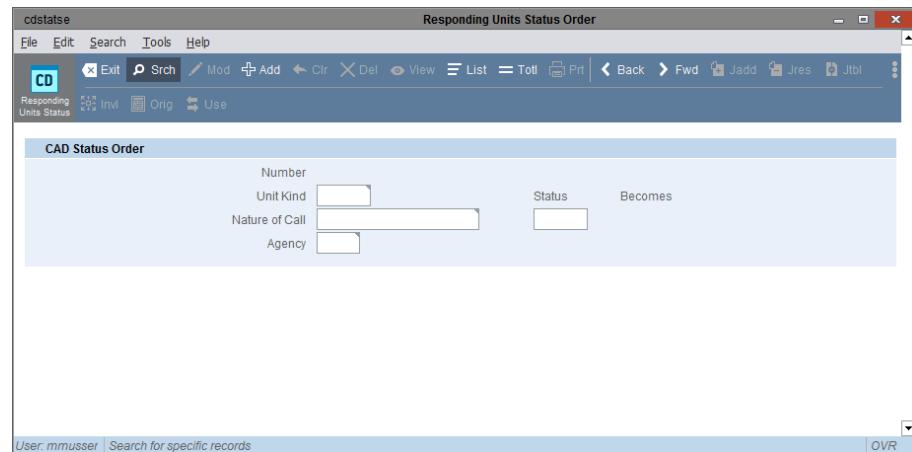
2. Click **Add**.

3. If the sequence is for a specific unit kind, then in the **Unit Kind** field, enter the code for the unit kind. For example, enter **LADD** for Ladder Truck.

4. In the **Nature of Call** field, enter **OneTouch**. This entry is case-sensitive.

A dialog box opens.

Yes/No Request	✕
❓ That value is not defined in tbnatur.abbr. Use anyway (Y/N)?	
Yes No	
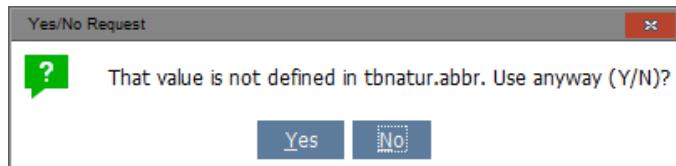
5. Click **Yes**.

6. If the sequence is for a specific agency, then in the **Agency** field, enter the agency code of the agency for which the sequence is being created.

7. In the **Status** field, click the **Detail** button.

   A detail window opens.

cdstatdt	✕
File Edit Search Tools Help	▲
✕ Exit 🔍 ✏ Mod ✚ Add ← ✕ Del 👁 ⋮	
Seq Status Becomes	
	▼
User: mmusser Add a new detail record OVR	
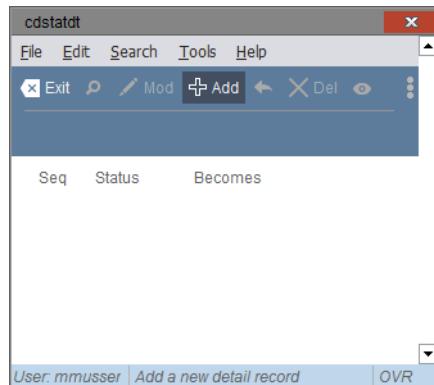
8. Click **Add**.

9. In the **Status** field, enter the status for the call as it appears in the Undispatched Calls window. For example, enter **RCVD** for Call Received.

10. In the **Becomes** field, enter the status for the unit to become. For example, enter **RCVD** for Call Received. For more information on setting up the **Status** and **Becomes** fields, see "Creating a status sequence for a unit" on page 71.

11. Repeat steps 8–10 for each status in the sequence.

    The status sequence for One-Touch Status buttons is created.

12. When finished, click **Exit** to close the detail window and return to the Responding Units Status Order table.

13. Repeat steps 2–12 for each unit kind or agency that needs a sequence for One-Touch Status buttons.

14. Click **Exit** to close the Responding Units Status Order table.

Understanding which Responding Units Status Order record is used

The One-Touch Status buttons are labeled according to records from the Responding Units Status Order table (`cdstatse`). The following table lists the logic used to determine which record is used.

Default order	Nature field	Unit Kind field	Agency field
1	`OneTouch`	Unit kind for the current user	Agency of the current user
2	`OneTouch`	(blank)	Agency of the current user
3	`OneTouch`	(blank)	(blank)
4	(blank)	Unit kind for the current user	Agency of the current user
5	(blank)	(blank)	Agency of the current user
6	(blank)	Unit kind for the current user	(blank)
7	(blank)	(blank)	(blank)

For example, by default, the software first looks for a `cdstatse` record with a **Nature** field value of `OneTouch`, a **Unit Kind** field value of the unit kind for the current user, and an **Agency** field value of the agency for the current user. If no such records exist, then the software looks for the values in the second default order. If no records exist that match the field values for default orders 1–6, then the software looks for the first `cdstatse` record where the **Nature**, **Unit Kind**, and **Agency** fields are blank.

Configuring the CAD filter

CAD calls can by filtered by agency, call type, zone, or unit so users see only the calls that they need to see. When the CAD filter is configured, the filter settings are applied to Voiceless CAD and Touch.

To configure the CAD filter:

1. At the command line, enter **adminutil**.

   The Administration Manager opens.

2. Select the **Settings** menu group, and then select the **All Settings** menu item.

3. Expand the **Module** folder, and then expand the **Module.CAD** folder.

4. Double-click the `MobileCADFilter` setting.

   A dialog box opens.
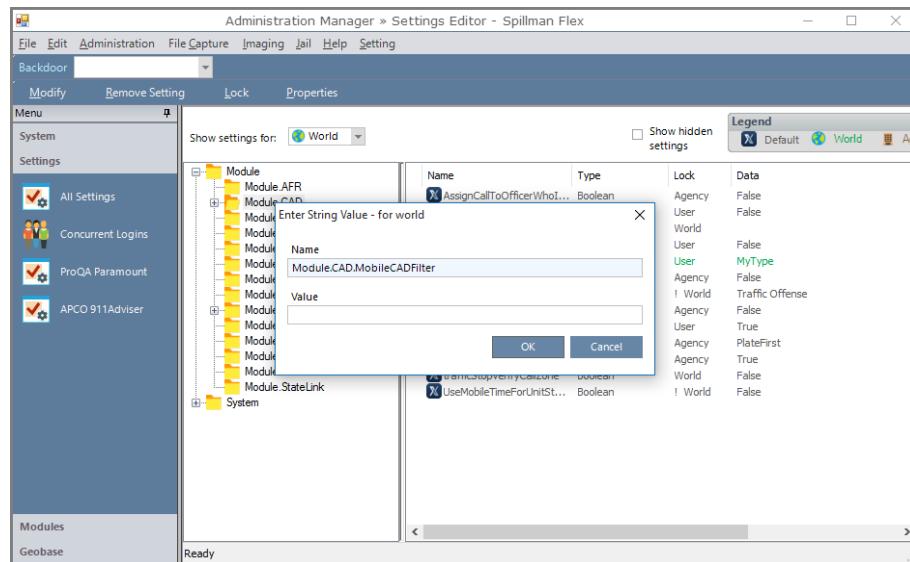
5. In the **Value** field, enter the desired filter value. For more information, see "Understanding CAD filter values" on page 85.

6. Click **OK** to close the dialog box and save the setting.

Understanding CAD filter values

This section describes the CAD filter values used for Voiceless CAD and the exceptions that might apply. Use the following table and the list of exceptions to determine what values to filter.

Value	Description
`MyAgency`	Displays calls and units within the user's agency.
`OtherAgency:`*`SPD,SFD`*	Displays calls and units within specified agencies. Enter the Agency Code value (`apagncy`) for the agencies to be displayed, separated by a comma. For example, if the codes are `SPD` and `SFD`, then enter **`OtherAgency:SPD,SFD`**.
`MyZone`	Displays call and units within the user's zone.
`OtherZone:`*`fwest,lne`*	Displays calls and units within specified zones. Enter the Zone Code value (`tbzones`) for the zones to be displayed, separated by a comma. For example, if the codes are `fwest` and `lne`, then enter **`OtherZones:fwest,lne`**.

Value	Description
MyType	Displays calls within the user's dispatch type.
OtherType:*f,e*	Displays calls and units within the listed dispatch types. Enter the dispatch types to be displayed, separated by a comma. For example, to display Fire and EMS dispatch types, then enter **OtherType:f,e**.
MyUnit	Displays calls assigned to the user's unit.
OtherUnit:*103,104*	Displays calls assigned to the listed units. Enter the Unit Number for the units to be displayed, separated by a comma. For example, to display units 103 and 104, enter **OtherUnit:103,104**.

Depending on their privileges, users can also filter their CAD data with custom filters and radio log history hours settings.

The following are CAD filter exceptions for units and calls. These filter exceptions cannot be changed, regardless of privileges granted.

CAD filter exceptions for units

For units, the following exceptions apply to the CAD filter:

- The user's unit is always visible, regardless of current status. The unit must have at least one Radio Log record. For more information, see the *CAD Administrator Manual*.

- Units with statuses that have not been updated within the value set in the `<RadioLogHistoryHours>` tag of the `options.xml` file are not visible.

- Units with the status of OFFDT are not visible.

- Units with a **Display flag** field value of 0 in the Units table (cdunit) are not visible, even with the status of ONDT.

- All units assigned to the current call of the user are always visible while assigned.

CAD filter exceptions for calls

For calls, the following exceptions apply to the CAD filter:

- Calls assigned to the user's unit are always visible.

- Calls for which the user's unit is set as the responsible unit are always visible, even if the unit is not currently assigned.

- Held calls are never visible.

Mobile Administrator Manual

Adding additional Mobile alert codes

The Alert Types code table (`mstbalrt`) contains the Attempt To Locate (ATL) and Be On The Lookout (BOLO) alert codes. Additional alert codes can be added for Mobile, if desired.

To add additional Mobile alert codes:

1. At the command line, enter **`mstbalrt`**.

   The Alert Types code table opens.
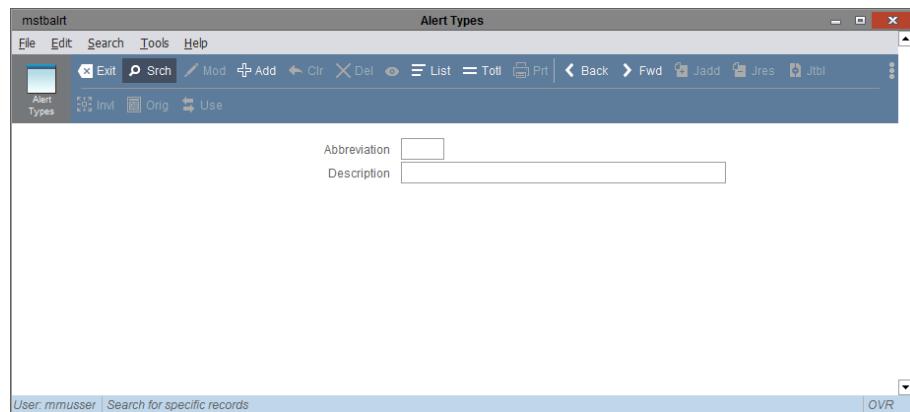
2. To search for a code, click **Srch**, and then enter your search criteria.

   Your first search result is displayed.

3. To see a list of results, click **List**.

   The list screen opens, listing all results matching your criteria.

4. Click the **Close** button to close the list screen and return to the Alert Types code table.

5. If the desired code was not listed, then click **Add**.

6. In the **Abbreviation** field, enter a code name for the alert. The field is alphanumeric, and can contain up to four characters.

7. In the **Description** field, enter a description for the alert. The field is alphanumeric, and can contain up to 15 characters.

8. Click **Accept**.

   The new code is added to the table.

9. Click **Exit** to close the Alert Types code table.

Managing the CAD Web Aggregator

CAD Web Aggregator settings can be managed in the Mobile WebApp Manager.

To manage the CAD Web Aggregator:

1. Log in to the Spillman Application Server. For more information, see the *Application Setup and Maintenance Manual.*

2. Double-click the **WebApp Manager** icon.

   The WebApp Manager opens.

3. In the **Application Manager** area, click the **/Mobile** link.

   The Mobile WebApp Manager opens to the Properties page.
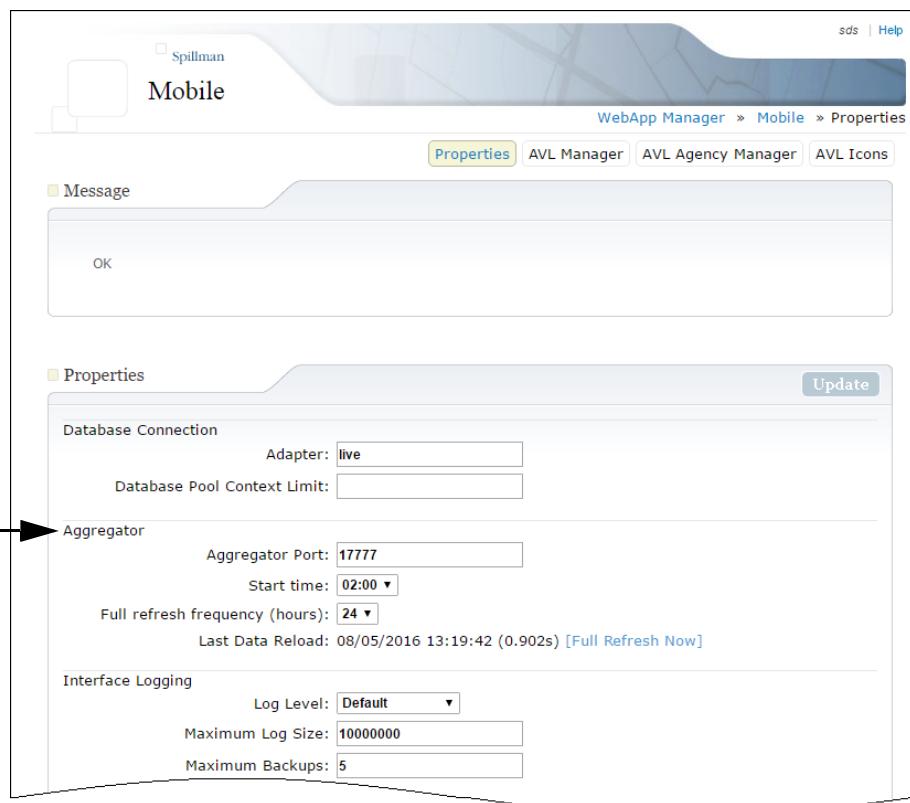
4. In the **Aggregator** area, change the Web Aggregator settings in the following fields as necessary:

   – **Aggregator Port**: Displays the port number for the aggregator. This setting is set in the `options.xml` file.

– **Start time**: Determines start time of the full refresh for the aggregator. The time is displayed in 24-hour format.

– **Full refresh frequency (hours)**: Determines how often the data is refreshed.

5. To immediately refresh the data for the CAD Web Aggregator, click the **Full Refresh Now** link.

6. When finished, close the browser to exit the WebApp Manager.

Setting CAD colors

The colors used in CAD to identify the status for calls and units are set in the Options dialog box.

To set CAD colors:

1. From the menu bar, select **File** > **Options**.

   The Options dialog box opens.
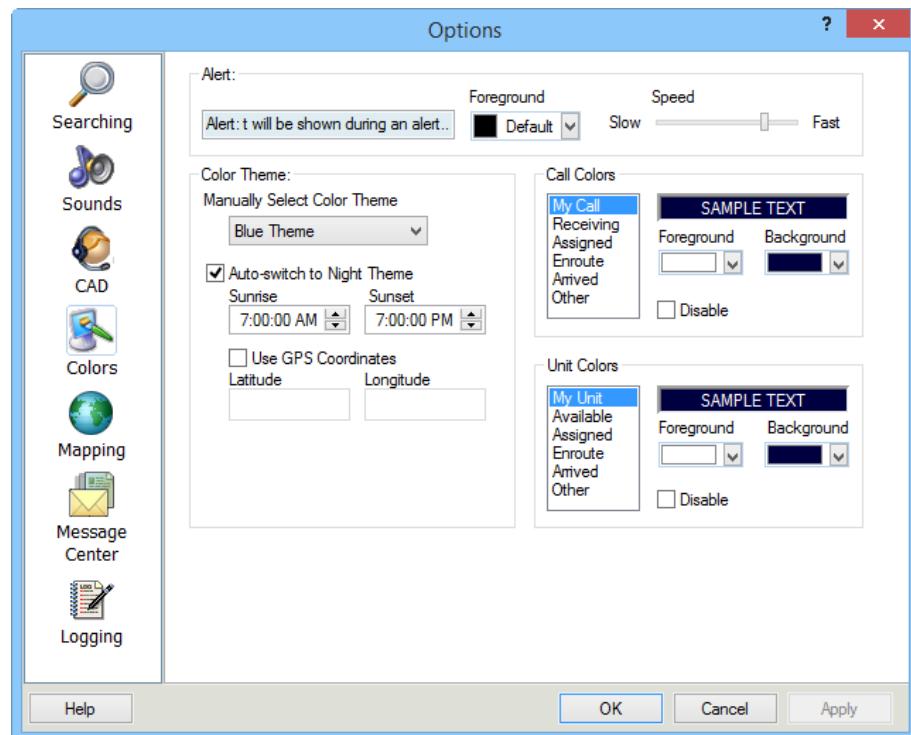
2. Click the **Colors** tab.

3. Do one of the following:

– To set the colors according to call type, in the **Call Colors** area, select the call type, and then use the drop-down lists in the **Foreground** and **Background** fields to select the foreground and background color for the call type. To use the color scheme specified in the **Other** option for all call types, select the **Disable** check box.

– To set the colors according to unit status, in the **Unit Colors** area, select the status type, and then use the drop-down lists in the **Foreground** and **Background** fields to select the foreground and background color for the unit status. To use the color scheme specified in the **Other** option for all statuses, select the **Disable** check box.

4. Click **OK** to apply your changes and close the Options dialog box.

5. If necessary, apply the settings to other users. For more information, see "Creating default settings for a group, agency, or all users" on page 55.

Managing CAD settings in the Administration Manager

Settings for Voiceless CAD are located in the Administration Manager. The following table describes the settings for Voiceless CAD in Mobile.

Setting	Description	Value
`ModifyCallLocation`	Determines whether users can modify the location of their call using Mobile. This setting can be set at a `World`, `Agency`, `Group`, or `User` level. • Set to **True** to allow users to modify the location of their call using Mobile. • Set to **False** to not allow users to modify the location of their call using Mobile. By default, the value is `False`. This setting is located in the **Module.MobileCallSettings** folder.	True/False
`ModifyCallNature`	Determines whether users can modify the nature of their call using Mobile. This setting can be set at a `World`, `Agency`, `Group`, or `User` level. • Set to **True** to allow users to modify the nature of their call using Mobile. • Set to **False** to not allow users to modify the location of their call using Mobile. By default, the value is `False`. This setting is located in the **Module.MobileCallSettings** folder.	True/False

Setting	Description	Value
`ModifyCallScope`	Determines whether only the call type for the assigned call is modified, or all call types attached to the call are modified. This setting can be set at a `World` or `Agency` level. • Set to **MT** to modify only the type for the call that is assigned to the responder. • Set to **MC** to modify all types attached to the call. • Set to **None** to not allow calls to be modified in Mobile. By default, the value is set to `None`. For multi-disciplinary agencies, it is recommended to set the value to **MT**. This setting is located in the **Module.MobileCallSettings** folder.	`MT/MC/None`
`OfficerUnitAssignmentStatuses`	Determines the list of unit statuses used to assign an officer to a unit during the login process. Set to the desired status, for example `ONDT`. The software clears the previously assigned officers from the unit and then assigns the current officer. The default value is `Empty`. This setting is located in the **Module.Mobile** folder. **NOTE**: For this setting to function, the following must be set up: • The `cdoffst` parameter must be specified. For more information, see the *CAD Administration Manual*. • The user must have the `mdcadmassignunit` privilege. For more information, see "Giving a user administrative access" on page 48.	`Unit Status 1/Unit Status 2/ Empty`
`UseMobileTimeForUnitStatusUpdates`	Determines whether the Mobile client time is used for radio log updates. • Set to **True** to use the client time for radio log updates. • Set to **False** to use the server time for radio log updates. By default, the value is `False`. This setting is located in the **Module.CAD** folder.	`True/False`
`AssignSelfAsResponsibleUnit`	Determines whether the **Become Responsible Unit** button is shown in Mobile, allowing an officer to self-assign as the responsible unit. This setting can be set at a `World`, `Agency`, `Group`, or `User` level. • Set to **True** to show the **Become Responsible Unit** button. • Set to **False** hide the **Become Responsible Unit** button. By default, the value is `False`. This setting is located in the **Module.CAD** folder.	`True/False`

Setting Up the Mapping Module

This section contains setup and maintenance information for the Mobile Mapping module. Before performing the administrative tasks in this section, complete the general setup tasks outlined in "Installation and Setup" on page 13.

This manual does not contain information on how to set up the Automatic Vehicle Location (AVL) module, which works with the Mobile Mapping module to display units on a map of your agency. For information on how to set up the AVL module, see the *Automatic Vehicle Location (AVL) Manual*.

If your agency has purchased the Mobile Mapping module, then the module is included as part of your Mobile installation.

To use Mobile Mapping, complete the following tasks:

- "Understanding the zoom factor" on page 92
- "Defining the vehicles to be displayed on the map" on page 93
- "Managing the directory location for your map files" on page 93
- "Configuring map layers" on page 95
- "Defining properties for layer components" on page 100
- "Determining the address settings of a street layer" on page 104
- "Working with orthophotographic layers" on page 106
- "Setting up the Mobile map to use hyperlinks" on page 106
- "Creating or saving a public configuration" on page 109

Understanding the zoom factor

The zoom factor determines which layers and labels are visible on the map at any one time. To see the current zoom factor, press Ctrl+Shift+Z. To increase the zoom factor, zoom in on the map. To decrease the zoom factor, zoom out on the map. Layers and labels can be assigned a minimum and maximum zoom factor. Layers with a zoom factor of 1 are always visible. For more information on setting the zoom factor of a layer, see "Setting the general properties for a layer" on page 98.

Use the following table to determine what each zoom factor displays on the map.

Zoom factor	Displays
1	The layer or labels
2	The layer or labels after the user zooms in one time
4	The layer or labels after the user zooms in two times
8	The layer or labels after the user zooms in three times
16	The layer or labels after the user zooms in four times
32	The layer or labels after the user zooms in five times
64	The layer or labels after the user zooms in six times

Defining the vehicles to be displayed on the map

In `cdunit`, any unit that is set up to use Mobile is displayed on the map. If your agency has additional units in which a GPS receiver is installed, then set up those units in `cdunit` as well. For more information, see . Units without a GPS receiver are displayed in the center of the zone to which they are assigned.

Managing the directory location for your map files

Map files can be saved to a directory on the network for all users to access, or the files can be saved to each computer that uses the Mobile map. If your agency's network is slow, then it is recommended to save the map files directly on each computer. For users with laptop computers, it is required to save the map files on each laptop computer.

Setting a directory location for your map files

Upon installation, all files for the Mobile map are placed in the following directory:

`C:\Program Files\Common Files\ESRI.`

It is recommended to use this location to save the map layer files. Create a folder called **Maps** at this location, and then copy your map files to the folder. If desired, your map files can also be saved at a different location, and the software can be configured to look for the map files at the set directory location.

After the map files are saved to the directory, set the directory location in Mobile.

To set the directory location for your map files:

1. From the menu bar, select **File > Options**.

   The Options dialog box opens.
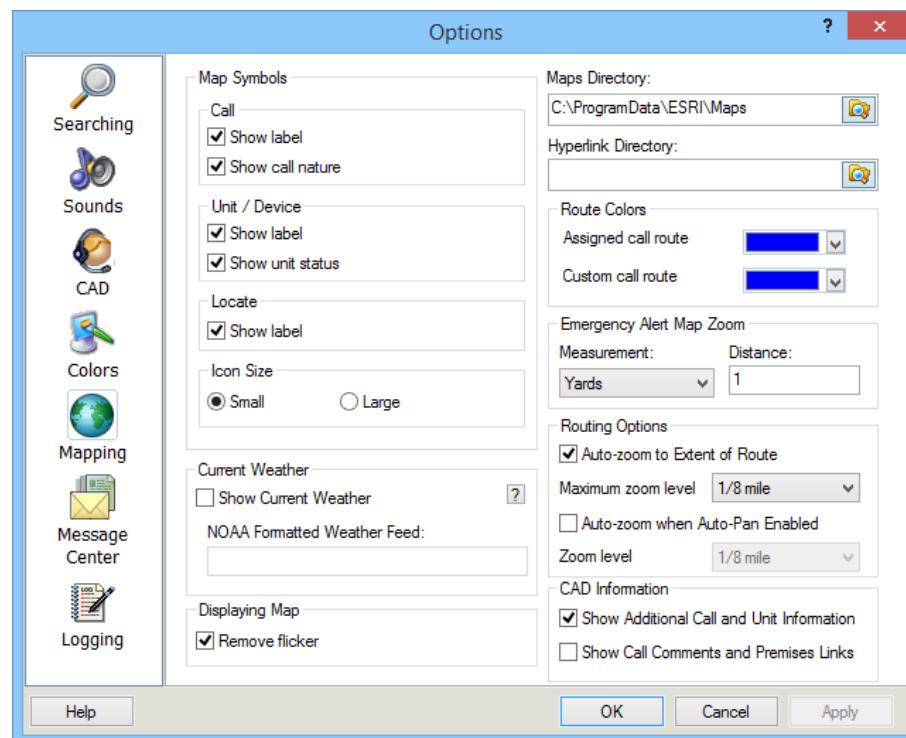
2. Click the **Mapping** tab.

3. In the **Maps Directory** field, click the folder icon.

   The Browse for Folder window opens.

4. Locate the directory in which the map files are stored, and then click **OK**.

   The directory location appears in the **Maps Directory** field.

5. Click **OK** to save your changes and close the Options dialog box.

6. If necessary, apply the settings to other users. For more information, see "Creating default settings for a group, agency, or all users" on page 55.

Synchronizing map files

Map files are synchronized with the specified directory location each time a user logs in to Mobile, so that the most recent files are always accessed. If your agency saves the map files to a directory on the network, then multiple directories can be created based on agency needs.

To create multiple directories on the server, use the following format:

- For all users: `$MOBILEDIR/uclient/all/maps/`

- For a state: `$MOBILEDIR/uclient/stateabbreviation/maps/`

- For an agency: `$MOBILEDIR/uclient/agencycode/maps/`

> **NOTE**
>
> The Agency code is the agency listed in the Units table (`cdunit`), not the agency in the Unit Status Backdoor table (`syunit`) or the Official Names Codes table (`apnames`). For UNIX and Linux users, the Agency code must be entered in lower case.
>
> For multi-server agencies, the uclient folder is created on the parent server, not on the individual agency servers.

- For an individual user: `$MOBILEDIR/uclient/username/maps/`

The maps directory specified in the Options dialog box is exempt from the automatic deletion that occurs when the server is synced with the client. If a file is removed from the server, but still exists in the specified maps directory, it is not automatically deleted from the client. Therefore, if a file is no longer required, it must be deleted manually. For more information on synchronization, see "Synchronizing client files" on page 42.

Configuring map layers

The layers used in Mobile map configurations must be saved as ESRI Shape files (`.shp`). Use Geographic Information System (GIS) software, such as ArcGIS, to convert map layers into ESRI Shape files. For more information, see your GIS documentation.

Completed map layers are used to create map configurations for your agency. To create a map configuration, use the **Layers** pane to add, rearrange or hide layers, and to view layer components.

The **Layers** pane is also used to define the properties of a layer. For more information, see "Defining properties for layer components" on page 100.

The following table explains the basic tasks that can be performed in the
Layers pane.

To	Do this
Move a layer to the foreground	Drag the layer to the top of the list in the **Layers** pane.
Show a layer	Select the check box next to the name of the layer.
Hide a layer	Clear the check box next to the name of the layer.
View the components of a layer	Click the plus sign next to the layer name.
Hide the components of a layer	Click the minus sign next to the layer name.

Adding and removing map layers

As many layers can be added to your map as desired, or layers can be
removed as needed.

> **CAUTION**
>
> Adding numerous layers or creating detailed layers increases the number of
> system resources your computer must use to properly display the map and might
> slow the performance of Mobile.

Adding a layer

To add a layer to the map:

1. From the Mapping toolbar, click **Layers** (Ctrl+L).

The **Layers** pane opens.

Layers button

Layers pane
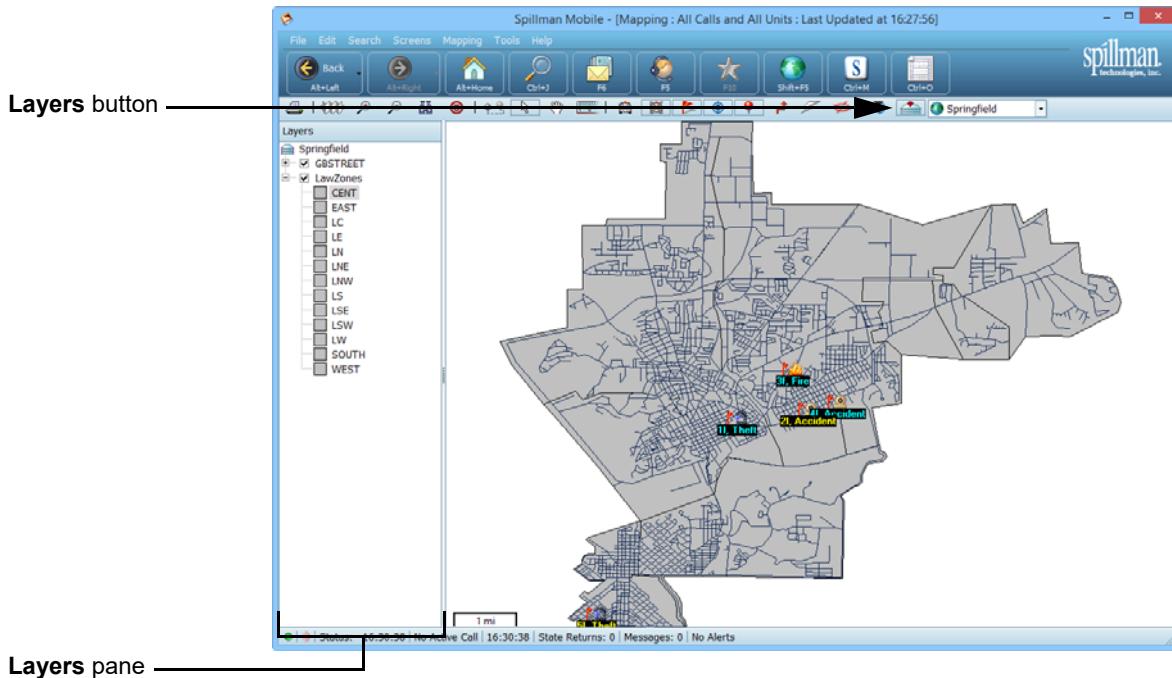
2. Right-click the configuration name (the default is **Layers**), and then select **Add Layer**.

   The Add Layer dialog box opens.

3. Navigate to the file location in which your map layers are stored, select the layer to add, and then click **Open**.

> **NOTE**
>
> By default, the type of layer to select is `.shp`. If an orthophotographic layer is being added, then select the type of orthophotograph being added from the file type drop-down list. For example, if your orthophotograph is a TIFF file, then select Tagged Image File Format (`.tiff`, `.tif`, `.tff`).

The layer is added to your configuration.

4. Save the configuration. See .

**Removing a layer**

To remove a layer from the map, from the Mapping toolbar, click **Layers** (Ctrl+L). The **Layers** pane opens. Right-click the layer, and then select **Remove**. The layer is removed from the map. When finished, save the configuration. For more information, see .

Setting the general properties for a layer

General properties set the name, visibility, and zoom factors for the layer.

To set the general properties for a layer:

1. From the Mapping toolbar, click **Layers** (Ctrl+L).

   The **Layers** pane opens.

2. Right-click the name of the layer, and then select **Properties**.

   The Layer Properties dialog box opens.
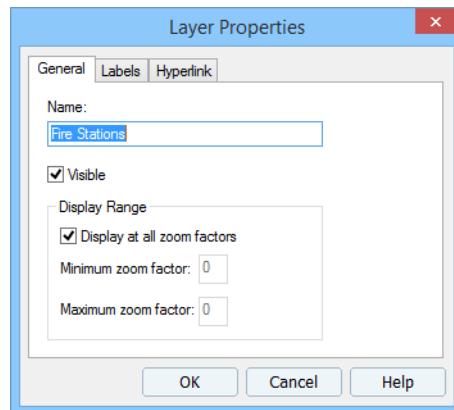
3. If necessary, click the **General** tab.

4. If desired, in the **Name** field, change the name of the layer to one that describes the layer, such as `Streets`, `Cities`, or `Zones`.

5. To show or hide the layer, select or clear the **Visible** check box.

6. In the **Display Range** area, do one of the following:

   – To use the default zoom factors, select the **Display at all zoom factors** check box.

   – To set the zoom factors, clear the **Display at all zoom factors** check box. In the **Minimum zoom factor** and **Maximum zoom factor** fields, enter the minimum and maximum zoom factor values.

> **NOTE**
>
> The zoom factor is the magnification that the map must exceed for the layer to appear on the map. For example, if a minimum zoom factor of `0` and a maximum zoom factor of `20` is entered, then the layer is not displayed after a zoom factor of `20` is exceeded. If a minimum zoom factor of `10` and a maximum zoom factor of `0` is entered, then the layer is displayed for all zoom factors above `10`.

7. Click **OK**.

   The Layer Properties dialog box closes and the changes are applied.

8. Save the configuration. See "Creating or saving a public configuration" on page 109.

Setting label properties for a layer

Label properties set the color and label names of the layer components in both the **Layers** tab and on the map. The zoom factor at which labels are displayed on the map is also set.

To set the label properties for a layer:

1. From the Mapping toolbar, click **Layers** (Ctrl+L).

   The **Layers** pane opens.

2. Right-click the layer name, and select **Properties**.

   The Layer Properties dialog box opens.
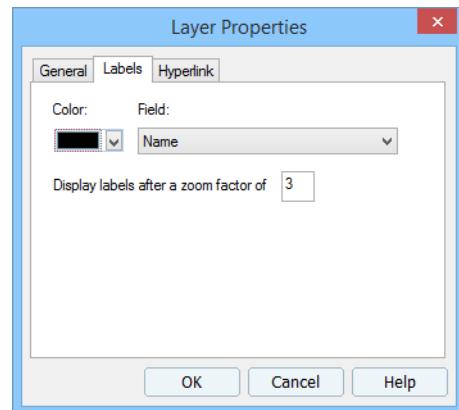
3. Click the **Labels** tab.

4. In the **Color** field, select a color from the drop-down list, or click **Other** to customize a color.

5. In the **Field** field, select the field whose value should be used as the label from the drop-down list.

> **NOTE**
>
> If a value is entered in the **Field** field, then labels can be quickly viewed for the specified layer on the map. To display the label, rest the mouse pointer on a map element on the layer. The label disappears when the mouse is moved or any key is pressed.

6. In the **Display labels after a zoom factor of** field, enter the zoom factor at which the label is displayed. See "Understanding the zoom factor" on page 92.

7. Click **OK**.

   The Layer Properties dialog box closes and the changes are applied.

8. Save the configuration. See "Creating or saving a public configuration" on page 109.

Defining properties for layer components

Layers are made of one of the following components:

- **Polygons.** Define a large area of the map, such as city codes and subdivisions.

- **Lines.** Define features, such as streets or rivers.

- **Points.** Define points on the map, such as landmarks or businesses.
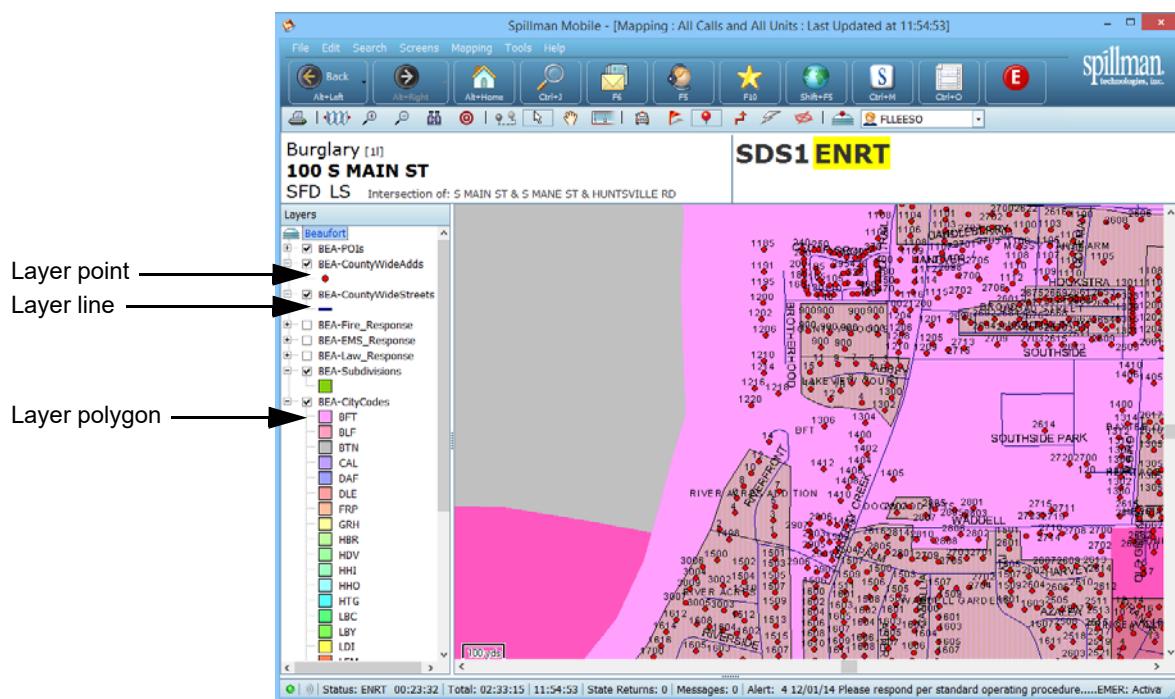
To define properties for specific layer components, complete the following tasks:

- "Defining properties for a polygon" on page 101

Defining properties for a polygon

The properties for up to 50 individual polygons per layer can be defined.

To define properties for a polygon:

1. From the Mapping toolbar, click **Layers** (Ctrl+L).

   The **Layers** pane opens.

2. Click the plus sign next to the layer that contains the polygon to define.

3. Right-click the polygon, and then select **Properties**.
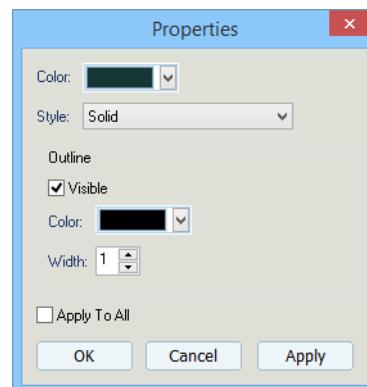
   The Properties dialog box opens.

4. In the **Color** field, select a color from the drop-down list, or click **Other** to customize a color.

5. In the **Style** field, select the pattern or style to use.

> **NOTE**
>
> If the `Transparent` style is used, then the background color of your map is used, and not the color specified in the **Color** field. If `Light Gray Fill`, `Gray Fill`, or `Dark Gray Fill` is specified, then the color selected in the **Color** field is formatted so that it can be seen through.

6. To display an outline around the polygon, in the **Outline** area, select the **Visible** check box and do the following:

– In the **Color** field, select a color from the drop-down list, or click **Other** to customize a color.

– In the **Width** field, select the width for the outline.

7. To apply the settings to all polygons in the layer, select the **Apply To All** check box. Otherwise, clear the check box to apply the settings to only the currently selected polygon.

8. Click **OK**.

   Your changes are applied to the map.

9. Save the configuration. See "Creating or saving a public configuration" on page 109.

Defining properties for all lines in a layer

To define properties for all lines in a layer:

1. From the Mapping toolbar, click **Layers** (Ctrl+L).

   The **Layers** pane opens.

2. Click the plus sign next to the line layer to define.

3. Right-click the line icon, and then select **Properties**.
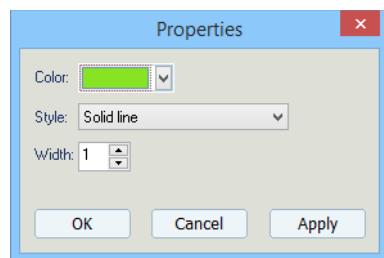
   The Properties dialog box opens.

4. In the **Color** field, select a color from the drop-down list, or click **Other** to customize a color.

5. In the **Style** field, select a line style from the drop-down list.

6. In the **Width** field, select a line width.

7. Click **OK**.

   Your changes are applied to the map.

8. Save the configuration. See "Creating or saving a public configuration" on page 109.

Defining properties for all points in a layer

To define properties for all points in a layer:

1. From the Mapping toolbar, click **Layers** (Ctrl+L).

   The **Layers** pane opens.

2. Click the plus sign next to the layer to define.

3. Right-click the point icon, and then select **Properties**.
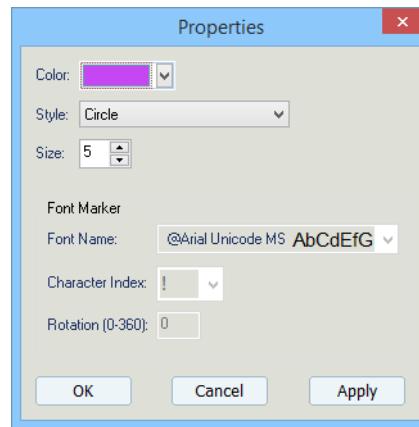
   The Properties dialog box opens.

4. In the **Color** field, select a color from the drop-down list, or click **Other** to customize a color.

5. In the **Style** field, select a point style from the drop-down list.

   – To use a font marker as a point icon, such as an icon for all homicides, select `True Type`. Continue to "Selecting a font marker" on page 103.

6. In the **Size** field, select the size for the point icon.

7. Click **OK**.

   Your changes are applied to the map.

8. Save the configuration. See "Creating or saving a public configuration" on page 109.

Selecting a font marker

With the Properties dialog box open for a point layer and `True Type` selected in the **Style** field, a font marker for a point icon can be selected.

To select a font marker:

1. In the **Font Marker** area, in the **Font Name** field, select the name of the font to use from the drop-down list.

2. In the **Character Index** field, select the font marker to use as the point symbol from the drop-down list.

3. To rotate the icon, in the **Rotation (0-360)** field, enter the number of degrees.

4. If necessary, in the **Size** field, change the font size.

5. Click **OK**.

   Your changes are applied to the map.

6. Save the configuration. See "Creating or saving a public configuration" on page 109.

Determining the address settings of a street layer

Use the Street Layer Settings dialog box to set the street layer settings so that the software can locate addresses on the map.

NOTE

Only one street layer can be set up in the Street Layer Settings dialog box. If this dialog box is used for multiple street layers, then the settings are applied only to the layer most recently set up.

To set the address settings for your street layer:

1. From the Mapping toolbar, click **Layers** (Ctrl+L).

   The **Layers** pane opens.

2. Right-click the configuration name, and then select **Street Layer Settings**.

The Street Layer Settings dialog box opens.

3. Complete the following:

   – **Street Layer** field: Select the street layer from the drop-down list.
     This list only contains line layers. If using more than one street
     layer, then select the primary street layer.

   – **Address Fields** area: Select a value from the drop-down list for
     each field to match them to the corresponding fields from your
     GIS software.

   – **Required Match Score (0-100)** field: Enter the value of tolerance
     to allow for address matches. A value of 100 requires a perfect
     match for the software to recognize the street. A value of 50–70 is
     considered a good match. Anything less than 50 is considered a
     poor match.

   – **Spelling Sensitivity (0-100)** field: Enter the value of tolerance to
     allow for spelling variations. The lower the value, the more
     variation the address locator allows. Using a lower value is
     recommended.

4. Click **OK**.

5. Save the configuration. See
.

Working with orthophotographic layers

Orthophotographs, such as aerial photographs or satellite images of your jurisdiction, are a type of raster that allows users to see map features that can provide additional information about a location. For example, if a dispatcher receives a call about an accident on a rural road next to a pond and a hill, then viewing an orthophotograph of the area can help the dispatcher pinpoint the location.

See your GIS documentation for a list of file types that are compatible with your GIS software.

Georeferencing an orthophotographic image in ArcGIS

If your agency uses ArcGIS and your orthophotographic image was not created with the same projection coordinates as your geobase (street) layer, then the projection coordinates for the image can be cleared and the image can be manually georeferenced to the geobase layer. Georeferencing allows the layer to be brought into alignment with an orthophotographic layer.

For more information, refer to your ArcGIS documentation, and the *Classic Geobase Administrator Manual*, *Geobase Administrator Manual*, or *GeoValidation Manual*, as appropriate for your software version.

Setting up the Mobile map to use hyperlinks

Hyperlinks can be added to points on the map to provide additional information, such as a map of a building or a photograph.

Hyperlinks can be created for point layers only. For more information on how to create hyperlinks for the map, see your GIS documentation. Once the hyperlinks are created, the Mobile map must be set up to use them.

To set up the Mobile map to use hyperlinks, complete the following tasks:

Adding hyperlinks

To show hyperlinks on the map, the hyperlinks must be added to features in the desired map service. The following instructions describe how to set up byperlinks for common places in ArcGIS. For more information, refer to your ArcGIS user documentation.

To add hyperlinks:

1. In ArcGIS, open the `.dbf` table for the point table to which hyperlinks will be added. For example, `Common Places`.

2. Click **Options**, and then select **Add Field**.

   The Add Field dialog box opens.

3. Complete the following fields:

   – **Name**: Enter **Hyperlink**.

   – **Type**: Select **Text** from the drop-down list.

4. If desired, in the **Field Properties** area, enter the number of characters for the field length. By default, the length is 50 characters.

5. Click **OK**.

   The **Hyperlink** field is added to the table.

6. In the **Hyperlink** field for the desired record, do one of the following to add a hyperlink:

   – Enter the directory path to the file. URLs can also be added.

   – If a directory location for all hyperlinks has been set, then enter a period and the unique portion of the path. For example, to link to a photograph that is stored in the directory named `LiquorStoreFire.jpeg`, enter **./LiquorStoreFire.jpeg**. To set a hyperlink directory location, see "Setting a directory path to hyperlink files" on page 108.

7. Repeat step 6 for each record in the table that needs a hyperlink.

8. When finished, save the changes to the table and exit ArcGIS.

Setting hyperlink properties for a layer

Hyperlinks can be added to a point layer only. Hyperlinks are used to display a link on the map to a directory location where files about the location on the map are saved, such as floor plans for a building.

To set the hyperlink properties for a point layer:

1. From the Mapping toolbar, click **Layers** (Ctrl+L).

   The **Layers** pane opens.

2. Right-click the point layer name, and then select **Properties**.

   The Layer Properties dialog box opens.
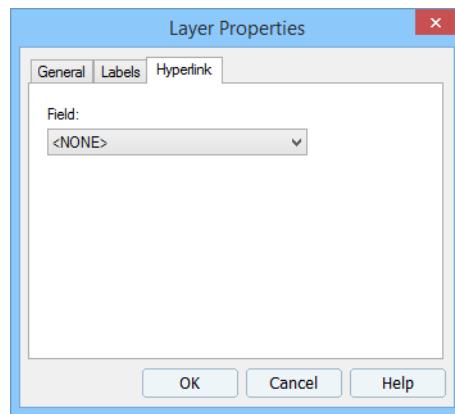
3. Click the **Hyperlink** tab.

4. In the **Field** field, select the name of the field that contains the hyperlinks from the drop-down list.

5. Click **OK**.

   On the map, the **Links** button is enabled. When the **Links** button is clicked, a yellow lightning bolt for each hyperlink is displayed on the map.

6. Save the configuration. See "Creating or saving a public configuration" on page 109.

Setting a directory path to hyperlink files

If your agency stores all the files to which hyperlinks are created in a central directory location, then the directory path must be set in Mobile. However, if your agency sets up dynamic hyperlinks, then this process is not needed.

To set the directory path to hyperlink files:

1. From the menu bar, select **File** > **Options**.

The Options dialog box opens.

Hyperlink Directory field
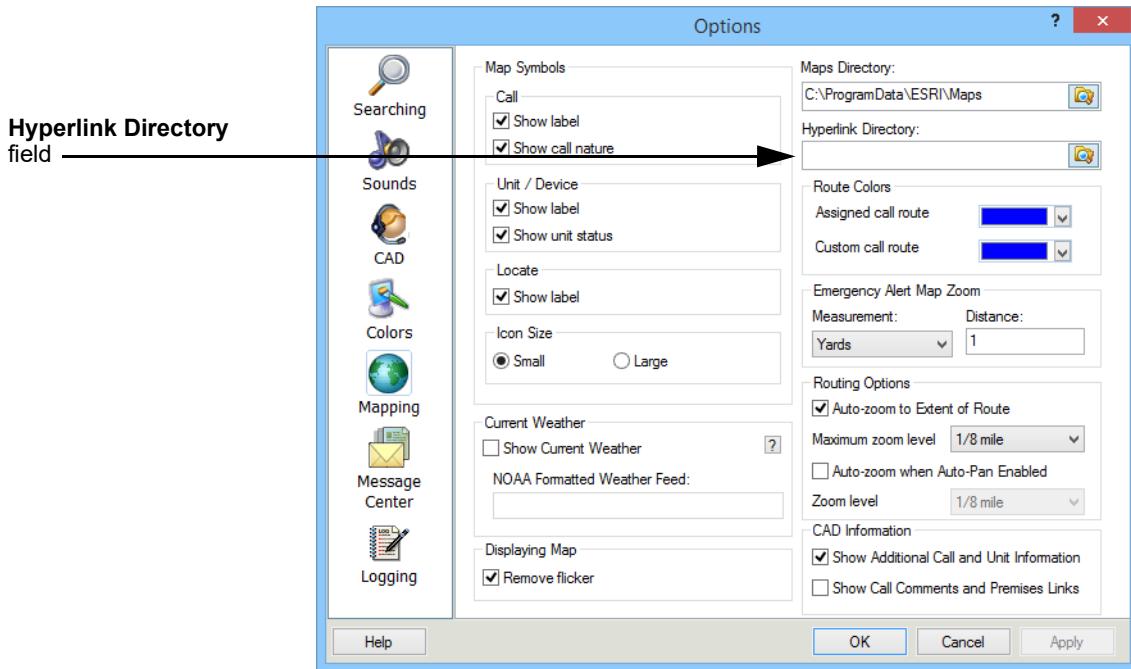
2. Click the **Mapping** tab.

3. In the **Hyperlink Directory** field, enter the directory path for your hyperlink files.

4. Click **OK** to close the Options dialog box and apply your changes.

5. If necessary, apply the settings to other users. For more information, see "Creating default settings for a group, agency, or all users" on page 55.

Creating or saving a public configuration

To create or save changes to public configurations for use by all Mobile Mapping users, Super User privileges are required.

To create or save a public configuration:

1. At the command line, enter **su**.

   Super User status is enabled.

2. From the Mapping toolbar, in the **Configuration** field, select a public configuration, and then click **Layers** (Ctrl+L). Public configurations are identified by a world icon.

The selected configuration is displayed on the map and the **Layers** pane opens.

3. Set the properties of the map configuration. Complete any of the following:

   – "Configuring map layers" on page 95

   – "Defining properties for layer components" on page 100

   – "Determining the address settings of a street layer" on page 104

   – "Working with orthophotographic layers" on page 106

   – "Setting up the Mobile map to use hyperlinks" on page 106

4. In the **Layers** pane, right-click the configuration, and then select **Save**.

   The Save As dialog box opens.

5. Do one of the following:

   – To save your changes as a new public configuration, enter a new name for the configuration, and then click **OK**. The new configuration is saved and appears in the **Configurations** field.

   – To save your changes and overwrite the existing configuration, click **OK** without changing the name of the configuration. A dialog box opens, asking if the existing configuration should be overwritten. Click **Yes**. The changes are saved to the configuration.

   If a user is set up to access the map directory on the network, then the changes are available the next time the user logs in to Mobile. If the map directory is set to a location on the individual's computer, then continue to step 6.

6. Copy all the map files that the configuration references and place them in the map directory for each user. For more information about creating map directories, see "Managing the directory location for your map files" on page 93.

   Once the files are placed in the directory, they are available for use.

Deleting a configuration

If a configuration is no longer needed, then it can be deleted.

To delete a configuration:

1. At the command line, enter **su**.

   Super user status is enabled.

2. From the Mapping toolbar, in the **Configuration** field, select a public configuration, and then click **Layers** (Ctrl+L). Public configurations are identified by a world icon.

   The selected configuration is displayed on the map and the **Layers** pane opens.

3. Right-click the configuration name, and then select **Delete**.

   A dialog box opens, asking to confirm if the configuration should be deleted.

4. Click **Yes** to delete the configuration.

   The configuration is deleted and is unavailable the next time users log in to Mobile.

Setting Up the Automated Field Reporting Module

This section contains setup and maintenance information for the Automated Field Reporting (AFR) module. Before performing the administrative tasks in this section, complete the general setup tasks outlined in "Installation and Setup" on page 13.

The Mobile forms in the Automated Field Reporting module are used to collect data while in the field. To use the Automated Field Reporting module, your agency must have purchased the Forms module. To use a Mobile form, Adobe Reader 9.4 or higher is required.

The tasks described apply only to the Automated Field Reporting module. If your agency uses the Mobile Field Report, Field Interview, or Arrest forms, then see the *Mobile Field Report and Forms Manual*. If your agency uses the State Crash and State eCitation forms, then see the *State Crash and State eCitation Forms Manual*.

To set up the Automated Field Reporting module, complete the following:

- "Customizing Spillman forms" on page 113
- "Setting up form privileges" on page 121
- "Syncing drafts" on page 122
- "Locking Mobile forms from future changes" on page 123
- "Setting up Workflow for electronic submission of state forms" on page 123
- "Understanding validation rules" on page 126
- "Using Mobile AFR forms with Night mode" on page 128

Customizing Spillman forms

Forms can be customized using the provided XML files. The following table lists the items that can be customized, the name of the XML file, and the default values.

Form item	File name	Default values
Heading images	`headingimages.xml`	By default, a heading image is not displayed in the form. To create a heading image, convert your agency logo to a compatible XML file and place it in the `headingimages.xml` file. For more information, see "Customizing heading images" on page 114.
Court and court-appearance date and time	`courts.xml`	By default, the tags in the `courts.xml` file are not set. Enter the values for your agency to automatically populate court appearance date and time information in the form. For more information, see "Customizing the courts.xml file" on page 116.
Report titles	`reporttitles.xml`	By default, the name for each generic form is listed under the `<ReportTitles>` tag. To change a form name, locate the tag for the form and change the values between the beginning and ending tags. For more information, see "Customizing form items" on page 118.
Agency and custom fields	`agencyfields.xml`	By default, the values in the tags in the `agencyfields.xml` file are blank. To create custom fields for your agency, locate the tags for the desired form and modify the values. For more information, see "Customizing form items" on page 118.
Eye color options	`eyecolor.xml`	The software uses the `tbcolor` code table for eye color, hair color, and vehicle color. This code file allows the eye color drop-down list to be limited to those colors that apply to eyes only. The software uses NCIC color values. For more information, see "Customizing form items" on page 118.
Hair color options	`haircolor.xml`	The software uses the `tbcolor` code table for eye color, hair color, and vehicle color. This code file allows the hair color drop-down list to be limited to those colors that apply to hair only. The software uses NCIC color values. For more information, see "Customizing form items" on page 118.

Form item	File name	Default values
Vehicle color options	vehiclecolor.xml	The software uses the tbcolor code table for eye color, hair color, and vehicle color. This code file allows the vehicle color drop-down to be limited to those colors that apply to vehicles only. The software uses NCIC color values. For more information, see "Customizing form items" on page 118.
Name involvements	nameinvolvements.xml	The software uses the sytbrshp code table to define a standard set of involvement types. These codes apply to various kinds of records. This code file creates a sub-set of involvement types that make sense for persons. For more information, see "Customizing form items" on page 118.
Property involvements	propertyinvolvements.xml	The software uses the sytbrshp code table to define a standard set of involvement types. These codes apply to various kinds of records. This code file creates a sub-set of involvement types that make sense for property. For more information, see "Customizing form items" on page 118.
Vehicle involvements	vehicleinvolvements.xml	The software uses the sytbrshp code table to define a standard set of involvement types. These codes apply to various kinds of records. This code file creates a sub-set of involvement types that make sense for vehicles. For more information, see "Customizing form items" on page 118.
Scars, marks, and tattoos category options	smt.xml	The software uses the nmtbnsmt code table for the NCIC set of codes for scars, marks, and tattoos. This code file adds categories to the standard sent of smt codes, helping the officer sift through the hundreds of available options. For more information, see "Customizing form items" on page 118.

Customizing heading images

To customize the images displayed in the form heading, the images must be converted to XML. Use the conversion tool Spillman provides to complete the process.

To convert an image to XML:

1. Open one of the following directories:

   – To update images for all agencies, open the file from

`$MOBILEDIR/uclient/all/fieldreports/codes`.

– To update the images for a specific agency, open the file from

`$MOBILEDIR/uclient/`*apagncy*`/fieldreports/codes`.

2. Open the `headingimages.pdf` file.

The file opens.
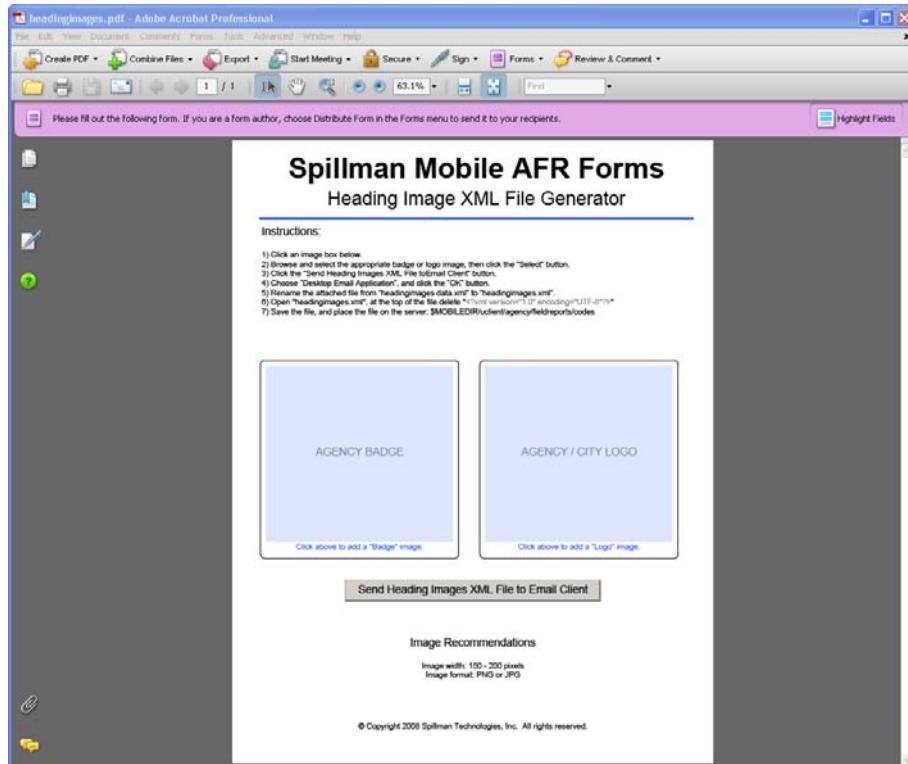
3. Follow the instructions on the form.

The file is converted and placed in the `headingimages.xml` file.

NOTE

If the `headingimages.xml` file is left blank, then no heading images are displayed in the forms.

Customizing the courts.xml file

The Spillman Citation AFR automatically calculates the court date and time based on the information provided in the `courts.xml` file.

> **NOTE**
>
> If the user does not select a court from the drop-down list, then the **You are hereby summoned to appear** area does not appear on the form.

To customize the `courts.xml` file:

1. Locate the folder containing the original file:

   `$MOBILEDIR/client/all/fieldreports/codes`.

2. Select the `courts.xml` file.

3. Copy the file to one of the following locations:

   – To update the `courts.xml` file for all agencies, copy to

   `$MOBILEDIR/uclient/all/fieldreports/codes`.

   – To update the `courts.xml` file for a specific agency, copy to

   `$MOBILEDIR/uclient/apagncy/fieldreports/codes`.

4. To customize the file, open it from the new location with a text editing program and complete the edits between the beginning and ending tags. Use the following table for reference.

XML Tag	Description
`<abbr>`	Enter the abbreviation for the court as it appears in the **Court Code** field of the Court Codes table (`tbcourt`).
`<desc>`	Enter a description for the court as it appears in the **Description** field of the Court Codes table (`tbcourt`).

XML Tag	Description
`<CourtName>`	Enter the name of the court as it should appear on the form in the **Courts** field drop-down list.
`<CourtCode>`	Enter a code for the court as it appears in the **Court Code** field of the Court Codes table (`tbcourt`).
`<CourtAddress>`	Enter the address for the court, including the street, city, state, and ZIP code. The values entered should match the values in the **Address** area of the Court Codes table (`tbcourt`).
`<CourtPhone>`	Enter the phone number for the court as it appears in the **Phone** field of the Court Codes table (`tbcourt`).
`<CourtStartTime>`	Enter the time the court opens in the 24-hour format, using the *hh:mm:ss* format.
`<CourtEndTime>`	Enter the time the court closes in the 24-hour format, using the *hh:mm:ss* format.
`<CourtDays>`	Enter the days of the week the court is in session. For example, if the court is open Monday through Friday, then enter **MTWHF**.
`<ProjectedDate>`	Enter the number of days from today's date that the offender should appear. This value is used in conjunction with the `<CourtDays>` value and the `<CourtHolidays>` value to determine the first available date to appear that court is in session. The last date to appear is automatically determined according to the requirements of your state.
`<CourtHolidays >`	Enter the date of the court holiday in the *mm/dd* format between the `<date>` beginning and ending sub tags. Enter each holiday as a new row under the `<CourtHolidays>` tag.

5. When finished, save your changes and close the file.

> **NOTE**
>
> If `<CourtStartTime>` and `<CourtEndTime>` are blank, then the **You are hereby summoned to appear** area does not contain the hours court is in session.

Customizing form items

Some default information, such as the values for vehicle color, involvements, or categories for scars, marks, and tattoos, can be customized. However, most agencies choose to use the default values.

To customize a form item:

1. Locate the folder containing the original file:

   `$MOBILEDIR/client/all/fieldreports/codes`

2. Copy the file to one of the following locations:

   – For all agencies:

   `$MOBILEDIR/uclient/all/fieldreports/codes`

   – For a specific agency:

   `$MOBILEDIR/uclient/`*apagncy*`/fieldreports/codes`

3. Right-click the file, and then select **Open with**. Select a text editor program such as WordPad to view the file.

   The file opens in the text editing program.

4. To customize an item, change the values between the XML tags. For example, to change the title of the General Use Law form, edit the values between the `<GeneralLawTitle>` beginning and ending tags.

5. Modify field attributes as needed. For more information, .

6. When all changes are complete, save your changes and close the file.

Setting field attributes and tags

Field attributes in the General Use forms can be set to accommodate the needs of your agency.

Use the following XML files to hide, disable, or make fields required:

- `accident-field-attributes.xml`
- `citation-field-attributes.xml`
- `field-interview-field-attributes.xml`
- `fire-field-interview-field-attributes.xml`
- `law-field-interview-field-attributes.xml`

▪ `warning-field-attributes.xml`

> **NOTE**
>
> Values for the < `Name`>, <`Location`>, <`ValueType`>, and <`Presence`> tags are case-sensitive.

Tags in the attributes.xml files

The following describes the tags that can be modified in the `attributes.xml`files.

`Name`

Determines the name of the field.

For example: <`Name`>`lawNature`</`Name`>

`Location`

Determines the location of the field in the form hierarchy using dot notation. Enter **[ ]** to indicate that this is a repeating field or fragment.

For example:

▪ <`Location`>`law.subLawDefault`</`Location`>

▪ <`Location`>`law.subLawMoreBody.offenses.offense[]`</`Location`>

▪ <`Location`>`names.name[].subNameDefault`</`Location`>

`ValueType`

Determines if the field is required or read-only. By default, the value is blank, which is the same as setting the value to `optional`.

If the field is set to `readOnly`, then the field appears the same as the other fields on the form, but cannot be edited.

For example:

▪ <`ValueType`>`optional`</`ValueType`>

▪ <`ValueType`>`required`</`ValueType`>

▪ <`ValueType`>`readOnly`</`ValueType`>

`Presence`

Determines if the field is displayed or hidden. By default, the value is blank,

which is the same as setting the value to `visible`.

> **NOTE**
>
> Setting the field to `disabled` might be preferable to `invisible`, since having several fields set to `invisible` could give the form an inconsistent visual layout. Disabling a field allows the form to retain its visual layout, but no longer allows direct interaction with the field.

For example:

- `<Presence>visible</Presence>`

- `<Presence>invisible</Presence>`

- `<Presence>disabled</Presence>`

`NumberRequired`

Determines how many repeatable fields are required. By default, the value is blank, which means only one repeatable field is required.

This tag applies to required fields only. If the field is not a repeatable field, then the value is ignored.

For example: `<NumberRequired>2</NumberRequired>`

`Message`

Determines the error message displayed when a required field is not completed. If the field is not required, then this value is ignored. By default, the value is blank, the cursor is placed in the required field, and the following message is displayed:

`A required field must be filled before saving the form`

For example:

`<Message>Please enter a Nature for this incident.
</Message>`

`!-- Display the More section of` *form* `--`

Determines if the More section of a form is displayed. Enter the tag before the `<Field>` tag for the form, were *form* is the name of the form.

Enter any of the following forms:

- Citation main form (`subCitationMoreBody`)

- Names subform (`subNamesMoreBody`)

- Vehicles subform (`subVehicleMoreBody`)

- Properties subform (`subPropertyMoreBody`)

- Signature subform (`subCitationSignature`)

- Notice subform (`subCitationNotice`)

For example:

```
<FieldAttributes>
        <FieldList>
<!-- Display the More section of Citation main form -->
            <Field>
                <Name>subCitationMoreBody<Name>
            </Field>
```

`!-- Hide` *Item* `Owner Information --`

Determines if owner information is displayed for a vehicle or property. Enter the tag before the `<Field>` tag for the `ownerInfo` field, where *Item* is either `Property` or `Vehicle`.

```
<FieldAttributes>
        <FieldList>
<!-- Hide Property Owner information -->
            <Field>
                <Name>ownerInfo</Name>
                <Location>properties.property[].
                subPropertyMore.subPropertyMoreBody
                </Location>
            </Field>
```

Setting up form privileges

To use the Mobile AFR forms, privileges must be granted in the Administration Manager (`adminutil`). For more information, see the *Security Setup and Maintenance Manual*.

System privilege	Description	Privilege
mdcmdlafracc	Grants access to use the General Use Accident form.	Access
mdcmdlafrcit	Grants access to the General Use Incident form.	Access
mdcmdlafrfi	Grants access to the General Use Field Interview form.	Access
mdcmdlafrfrfi	Grants access to use the General Use Fire Field Interview form.	Access
mdcmdlafrfrwarn	Grants access to the General Use Warning form.	Access
mdcmdlafrlaw	Grants access to the General Use Law form.	Access

Syncing drafts

Form drafts saved from the Mobile client are sent to the server for synchronization when a connection is available.

Once drafts are saved in the msmain table (`msmain`) or the Messenger Messages table (`msdata`), they are sent to the client in the same manner as other messages.

In addition to caching forms on the client in the `%APPDATA%` system folder, then the client synchronizes drafts to the server the next time a connection is available. Once a draft is created, if a connection is available during that session, the client saves the draft to the server in the background, otherwise, the draft is saved the next time the user logs in to Mobile.

Mobile synchronizes drafts saved on the server by comparing server values with the local draft cache (`drafts.xml`). Any new or updated drafts coming from the server are directed into the local cache. The client keeps track of whether the draft is synchronized with the server by the `<isOnServer>` attribute of the item tag in `drafts.xml`, so that it can send the draft to the server at any time.

In the **Drafts** folder of the Message Center, synchronized drafts are signified by a green check mark icon, and can be accessed from any computer on the network. Drafts that are saved to the client only are signified by a red void icon.

Drafts are stored on the server in `msmain` or `msdata` with the extension type `.draft`.

Finding drafts associated with a user

To find drafts associated with a user:

1. Open the `msmain` table.

2. In the **Type** field, enter **draft**.

3. In the **Response Recipient** field, enter the user name for the user.

4. Click **Accept**.

    A search is performed for records matching your criteria. One of the following occurs:

    – The first matching result is displayed. Continue to step 5.

    – If no results are found, then a message box opens stating that no matching records are found. Click **OK** to close the message box.

5. To list your results, click **List**.

    A list screen opens and the records are displayed.

6. Select the desired record, and then click **Accept**, or double-click a record to open it.

7. When finished, click **Exit** to close the table.

Locking Mobile forms from future changes

Use the `lockform` application parameter to lock a form from future changes based on workflow status. The following table describes the `lockform` application parameter.

Parameter	Description	Value
`lockform`	Determines whether a form is locked from future changes after the form is saved. Set the value to any workflow statuses which should be locked from changes, separated by a comma. For example, to lock all forms with the status of COMPLT or REMIT, set the value to **COMPLT, REMIT**.	Any workflow status

Setting up Workflow for electronic submission of state forms

Depending on the requirements for your state, some forms can be submitted to the state electronically. For more information on setting up Workflow, see the *Application Setup and Maintenance Manual*.

Use the following as a guide to set up workflow for electronic submission of state forms. Depending on the needs of your agency, your actual field values and the number of status entries might vary.

To set up Workflow for electronic submission of state forms:

1. In the Workflow Status Configurations screen (`wfstatcf`), add a new workflow status entry for inputting information into a record and rerouting a failed submission.

2. Complete the **Workflow Status Configurations** area as appropriate for the agency and form.

3. In the **Status Code Sequence** area, click **Detail**.

   A detail window opens.

4. Add the first workflow status. Complete the following fields:

   – **Abbr**: Leave this field blank.

   – **Description**: Enter **No Status**.

– **Action**: Enter **1**. The value entered must be positive.

– **Next Status**: Enter **INPUT**.

5. Add the next status. Complete the following fields:

– **Abbr**: Enter **INPUT**. This value must match the value entered in the Next Status field in step 4.

– **Description**: Enter a description for the status, such as **Input Information into Record**.

– **Action**: Enter **1**. The value entered must be positive.

– **Next Status**: Enter **SENDST**.

6. Add the next status. Complete the following fields:

– **Abbr**: Enter **SENDST**. This value must match the **Next Status** field value entered in step 5.

– **Description**: Enter a description for the status, such as **Send to State**.

– **Action**: Enter **-1**. The value entered must be negative. If an error is returned from a state submission, this tells the software to use the status prior to SENDST as the new status for the submission.

– **Next Status**: Enter **COMPLT**.

7. Add the final workflow status entry for workflow completion. Complete the following fields:

– **Abbr**: Enter **COMPLT**. This value must match the Next Status field value entered in step 6.

– **Description**: Enter a description for the status, such as **Workflow Completed**.

– **Action**: Enter **0**.

– **Next Status**: Enter **COMPLT**.

8. Click **Accept** to accept your changes.

9. Click **Exit** to close the detail window and return to the Workflow Status Configurations screen.

10. Click **Accept** to save the record.
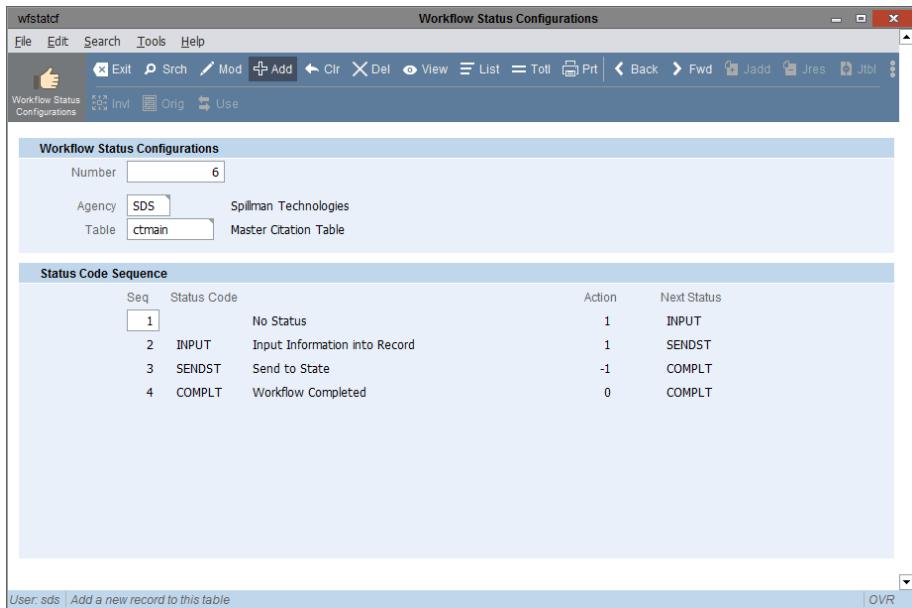
If a submission is successful, then the workflow is moved to the next workflow status, in this example `COMPLT`, and the assignee is unchanged.

If a submission fails, then it is moved back to the previous workflow status, in this example `INPUT`, and assigned to the person who received the response from the state.

The response from the state is displayed in the comments section of the workflow. The response is also displayed in the **State Returns** folder for the user in the Message Center.

Errors, warnings, and messages returned from the state are sent to the user, who corrects the problem and resubmits the form.

Understating the Law Supplement form and workflow

The Law Supplement form generates a Law Supplement workflow, and not a Law workflow with the attached form and all supplements. The Law Supplement workflow attaches only the Law Supplement form being added or

modified and links directly to the Supplement record, bypassing the Law record. The Law form and workflow is not affected and continues to attach all supplements.

> **NOTE**
>
> A Law Supplemental Narrative record is created in the Law Supplemental Narrative table (`lwsupl`) regardless of whether the narrative was filled out in the form. For example, if an officer opens a new Law Supplement form and adds an additional name but no narrative, then a Law Supplemental Narrative (`lwsupl`) record is created with an empty narrative. The name on the form is linked to the Law record through an involvement.

Understanding validation rules

The goal of the validation rules is to avoid creating duplicate records that will have to be merged at a later time. Without biometric identifiers, such as finger prints, it is not possible to guarantee that a match is always correct.

In addition to validation rules, either the incoming form data can be trusted, or the database can be preserved and all incoming changes can be inserted into the narrative and comments. This option is set on the Data Exchange (DEx) Properties page. For more information, see the *DEx Interface Setup Manual*.

Mobile AFR forms have specific fields that must be populated for a valid record to be added or modified in the database. When the actual record number is not known, these specific validation fields are used to match on existing records. If no matches are found, then a new record is added.

The following table lists the attempted record type and the specific fields that must be populated for a valid record to be added or modified in the database. An asterisk (*) indicates that an exact match is required.

Attempted record	Fields validated	Additional information
Name (Alias)	• Key (Name Number) • Last Name + First Name + [Middle Name*] + [Suffix*] + Alias Number	If a suffix is entered and it is different than the existing record, then the attempted record is not considered a match and a new Name record is created. The software validates against full middle names only. If a partial match is detected, then the longest middle name is retained.
Name (Type)	Last Name + [First Name*] + [Middle Name*]	There are additional validation rules for business names. Business names do not always contain a first name. If the Name Type is anything other than `Individual`, then the fields listed are used to validate against existing records. If no matches are found, then a new record is added.
Name	• First Name + SSN • First Name + DL Number + DL State • First Name + Last Name + [Middle Name*] + [Suffix*] + DOB • First Name + Last Name + [Middle Name*] + [Suffix*] + Home Phone • First Name + Last Name + [Middle Name*] + [Suffix*] + Address • A Name record with a matching middle name	If the **Address** field value is validated, then the address must match the **Street**, **City**, **State**, and **ZIP** values exactly with no additional spaces, capitalization, or punctuation differences of any kind.
Vehicle	• VIN • License Number + License State • License Number + License State + Make + Model + Year	Make, Model, and Vehicle Year are validated only if the **Include Make/Model/Year** check box is selected in the DEx Properties page. By default, the check box is not selected. For more information, see the *DEx Interface Setup Manual*.
Property	• Add: Item + Brand + Model + Serial Number • Modify: Key (Property Number) or Match on Add Rule	Not applicable.

Attempted record	Fields validated	Additional information
Law, Citation, Warning, Field Interview, or Fire Field Interview	Key	Key types: • Law: Incident Number • Citation: Citation Number • Warning: Warning Number • Field Interview: FI Number • Fire Field Interview: FRFI Number
Accident	• Key (Accident Number) • [Related By Incident Number*]	Not applicable.

Using Mobile AFR forms with Night mode

Mobile AFR forms are not controlled by Night mode. To display a form in a way similar to Night mode, adjust the settings in Adobe Reader to the desired colors. For more information, see the Adobe Reader user guide.

Using the Translation Administration Tool

The Translation Administration Tool is a web application that allows administrators to add, edit, and delete translation codes from a centralized location. Translation codes translate values from state returns to table values used in the database records, and from database records to values the state uses.

Use the Translation Administration Tool to do the following:

- Customize translation codes without editing raw XML files.
- Import translation codes as a Comma Separated Values (CSV) file.
- Send automated emails to the SAA when it is found that a translation code is missing.

The Translation Administration Tool is located on the Spillman interfaces-server and provides the following:

- Remote access capability to the web application from a tablet or computer without the software.
- The ability to grant additional users access based on existing manager groups.
- Immediate changes to the translation tables when the web application is restarted.

Configuring the Translation Administration Tool

To configure the Translation Administration Tool:

1. Open a web browser, and in the **Address** bar, enter the following:

   `http://`*`ServerName`*`:4081/TranslationAdmin`

   where *ServerName* is the name of your agency server.

2. When prompted, enter your user name and password.

The Translation Admin Tool screen opens to the Configuration page.

NOTE

Initial configuration is required when logging in for the first time only. For subsequent sessions, the Navigation page opens after logging in.

3. In the **State** field, select your state, and then click **Continue**.

The Navigation page opens.
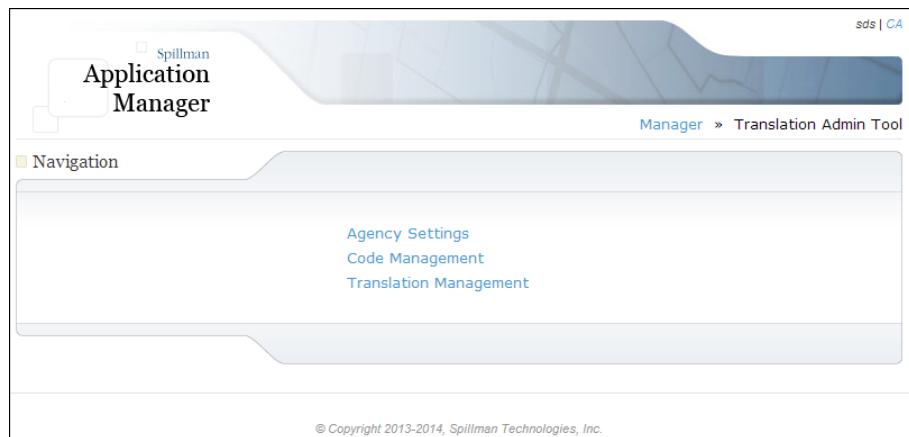
4. Configure the following settings by clicking the corresponding link:

   – **Agency Settings**: Used to configure settings for agencies connected to the server. See "Using the Agency Settings screen" on page 131.

   – **Code Management**: Used to compile lists of known codes for the state. See "Using the Code Management screen" on page 134.

  – **Translation Management**: Used to manage the translation of Spillman codes to the state codes listed in the Code Management screen. See "Using the Translation Management Screen" on page 142.

5. When finished, close the browser to exit the Translation Administration Tool.

Using the Agency Settings screen

The Agency Settings screen is used to configure settings for agencies connected to the server.
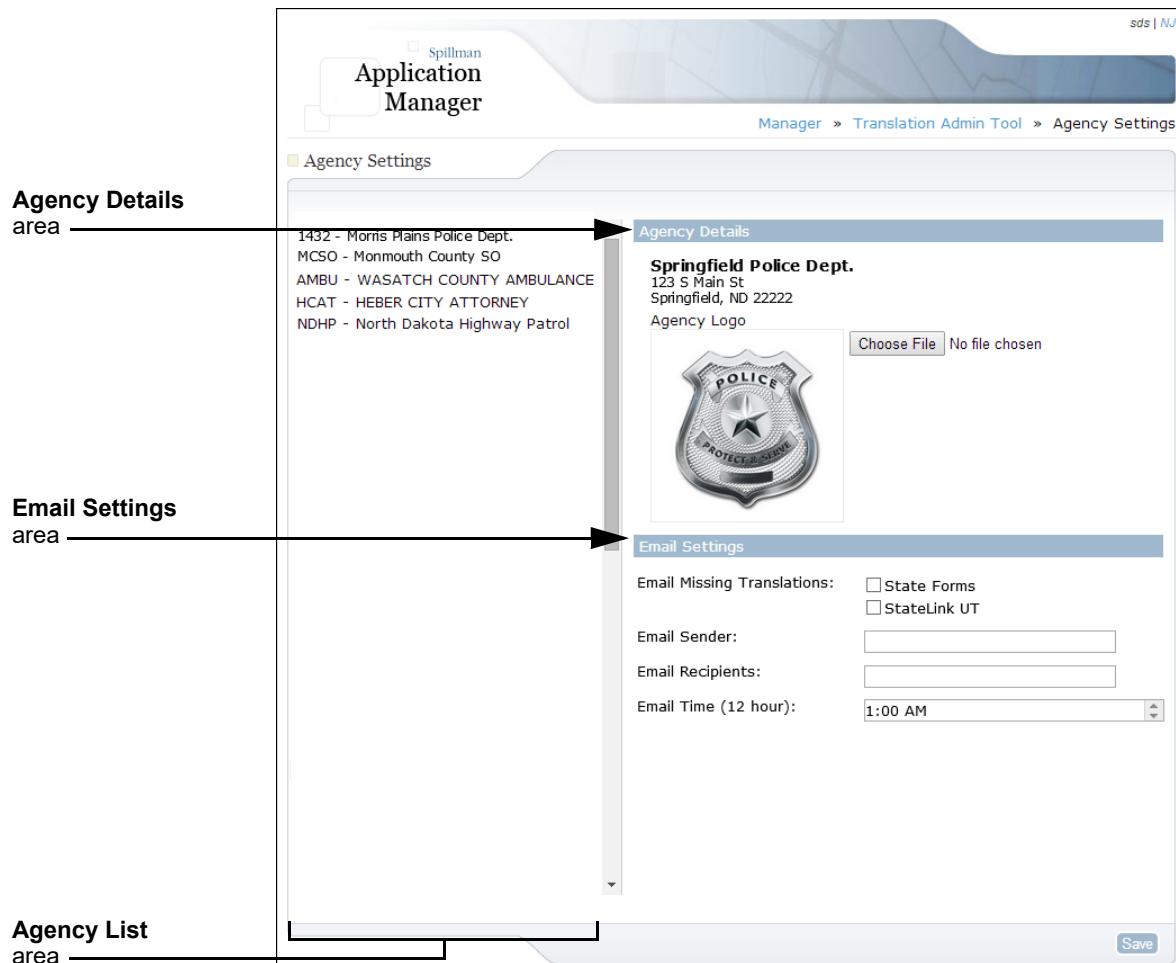
The Agency Settings screen is organized into the following areas:

▪ **Agency Details.** Displays basic agency contact information, and is used to change the agency logo.

▪ **Email Settings.** Used to configure the settings for users to receive notifications if there is a field value found in a submitted form that lacks a translation or when a user imports a state return and there are values that are not translated. Users can select the types of translations for which they would like to receive an email.

▪ **Agency List.** Displays values from the Agency Codes table (`apagncy`).

Configuring agency settings

Use the Agency Settings screen to configure settings for agencies connected to the server.

To configure settings for an agency:

1. From the Agency Settings screen, in the **Agency List** area, select the agency to configure.

2. In the **Agency Details** and **Email Settings** areas, complete the fields. For field descriptions, see "Agency Settings field descriptions" on page 132.

3. Click **Save**.

Agency Settings field descriptions

The following lists fields in the Agency Settings screen.

`Agency Logo`

To upload an agency logo, click **Choose File**, and then select the image file to display on the Agency Settings page. Logos can be Graphics Interchange Format (.gif), Joint Photographic Experts Group (.jpg), or Portable Network Graphics (.png) files. It is recommended to use a .png file for a transparent background. The logo is saved to the uclient, and creates or replaces the logo added to agency forms reports or used in various parts of the software. This field is optional.

`Email Missing Translations check boxes`

Select the check box for the report that will be sent to the specified email recipients. This field is required and multiple reports can be selected.

`Email Sender`

Enter the email address to use to send the notifications that translation codes are missing from a table. This field is required.

`Email Recipients`

Enter the email address to use as the recipient for notifications that translation codes are missing from a table. To enter multiple email addresses, separate each with a semicolon followed by a space.

For example, enter **`Name1@spillman.com; Name2@spillman.com`**.

This field is required.

`Email Time (12 hour)`

Enter the time to send out notifications that translation codes are missing from a table in *hh:mm AM/PM* format. This field is required.

Using the Code Management screen

The Code Management screen is used to create lists of state codes the agency will use in the Translation Management screen.
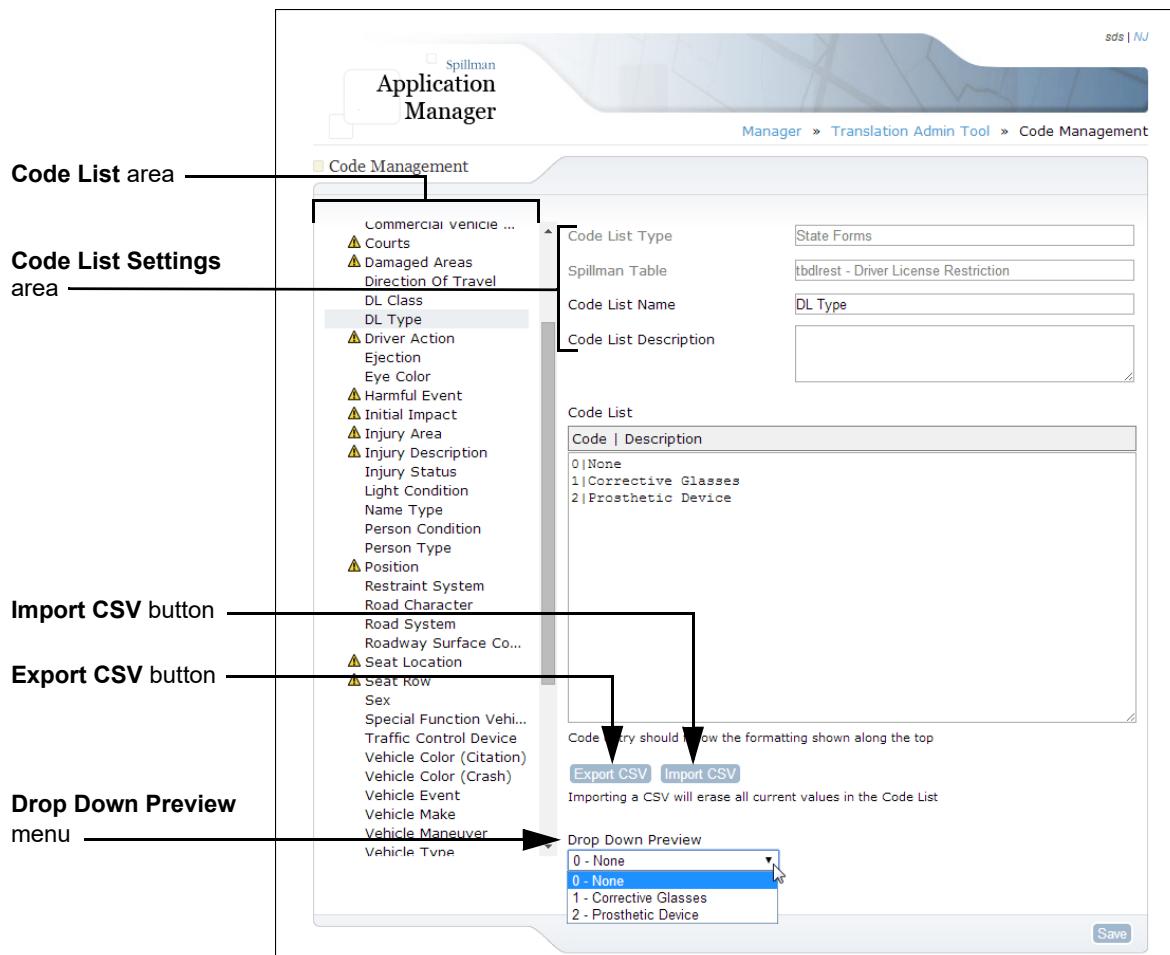
The Code Management screen is organized into the following areas:

- **Code List.** Displays the available code lists and is organized by State Form codes and StateLink codes. A caution icon indicates that the specified code list has no values.

> **NOTE**
>
> To add or remove code lists from the **Code List** area, contact Spillman Technical Services.
>
> Depending on your state requirements, the following code lists are read-only and cannot be edited:
>
> – Alcohol Drug Test Status
> – Alcohol Test Type
> – Commercial Vehicle Weight
> – Person Type
> – Eye Color
> – Sex

- **Code List Settings.** Displays the settings for the selected code list.

- **Code List text box.** Displays the state code and description. Header information displayed in the **Code List** header and text box changes based on the list type selected. For example, for a `State Forms, Road System` code list, the header may display as the following:

  `Code | Description`

Adding and editing officer names in the Names code list

The Names code list contains the names for the officers in your agency. Officer names can be imported from your database to match the requirements of the State eCitation or State Crash form for your state. For more information on setting up the State eCitation and State Crash forms, see the *Mobile State eCitation and State Crash Forms Manual*.

To import officer names:

1. From the **Codes List** area, select **Names**.

The Names code list opens.

2. Click **Import From Database**.

The Please select the desired parsers dialog box opens.

3. Do any of the following:

– To overwrite the current data in the Name code list, select the **Overwrite all existing data** check box.

– To determine how the first name is displayed, in the **First Name parser** field, select the desired format from the drop-down list. For example, to display only the first initial of the first name, select `First Name Initial`.

– To determine how the last name is displayed, in the **Last Name parser** field, select the desired format from the drop-down list. For example, to display the full last name, select `Last Name Full`.

4. When finished, click **Submit**.

   The officer names are imported from the Official Names Codes table in your database with the specified format.

5. Click **Save** to save your changes.

Editing the Names code list

Once the Names code list is populated, the contents can be edited as needed, or new names can be added.

To add a new name, in the **Code List** text box, enter the name on a new line using the following format:

Code | Description | First | Middle | Last

where *Code* is the **Name Code** field value from the Official Names Codes table, *Description* is the **Officer Name** field value from the Official Names Codes table, *First* is the first name of the officer, *Middle* is the middle name of the officer, and *Last* is the last name of the officer.

If no information should be entered for a value, then leave the space between the pipes for that value blank. For example, to add David Gordon with no middle name, enter the following:

`101| D Gordon | David || Gordon`

To modify the Names code list, in the **Code List** text box, edit the information between each set of pipes (|) as needed. For example, if no last name was imported, but a last name is needed, then to add a last name, enter the name between the pipes for the last name.

To save changes made to the Names code list, click **Save**.

Creating a state code list

Use the Code Management screen to create a list of state codes for an agency.

To create a list of state codes for an agency:

1. From the **Codes List** area, select a code list to edit.

2. In the **Code List Settings** area, modify the field settings as needed. The following fields are in the **Code List Settings** area:

   – **Code List Type**: Displays the type of list selected. For example, `State Forms`. This field is read-only.

   – **Spillman Table**: Displays the Spillman table name that corresponds to the code list. This field is read-only.

   – **Code List Name**: Displays the name of the selected code list. This field can be modified, if desired.

   – **Code List Description**: Provides information about the code list, such as which box on the state form the codes come from, and the location where code values are saved. This field can be modified, if desired.

3. In the **Code List** text box, modify the code and description values to match values from state forms and state returns.

4. If your state provides codes in a CSV file, click the **Import CSV** button.

   The Choose File to Upload dialog box opens.

5. Select the CSV file, and then click **Open** to upload the values in the CSV file to the **Code List** text box.

> **NOTE**
>
> Code lists can also be exported as CSV files to share with other agencies or to back up your codes. To export a code list CSV file, select the code list from the **Codes List** area, and then click the **Export CSV** button. Save the code list in the file location of your choice, and then distribute the list as desired.
>
> If your agency imports statutes from StateLink, then see .

6. To see a preview of the list as it will appear in the Translation Management screen, in the **Drop Down Preview** field, click the field to review the drop-down list.

7. When finished, click **Save**.

Importing statutes from StateLink

For some states, the Statutes code list is updated by importing the statutes from StateLink.

To import statutes from StateLink:

1. In the **Codes List** area, select **Statutes**.

The Statutes code list opens.
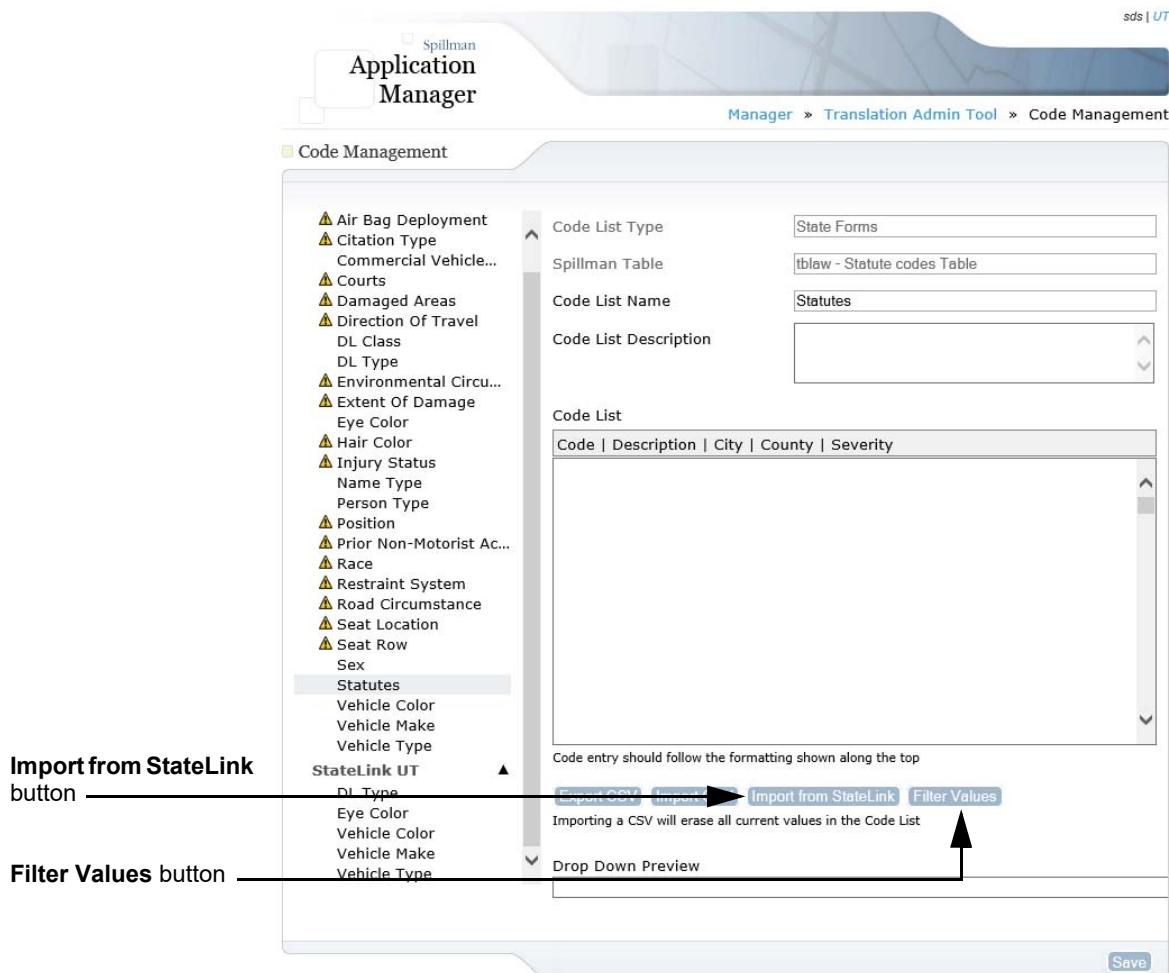
2. Click **Import from StateLink**.

The Please enter your StateLink Credentials dialog box opens, and the **Web Service Address** field is populated with the URL from which the statutes are imported.
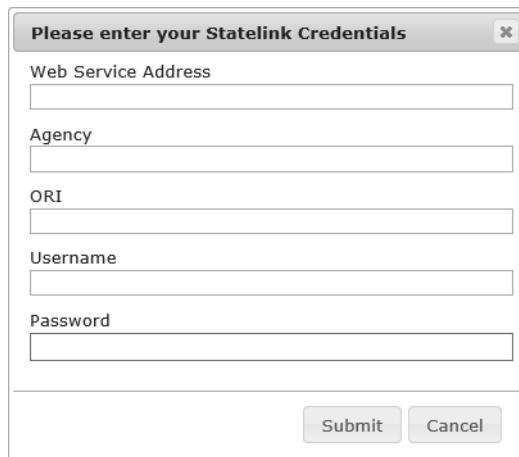
> **NOTE**
>
> For help with the **Web Service Address** field, contact Spillman Technical Services.

3. Complete the following fields:

   – **Agency**: Enter the name of your agency.

   – **ORI**: Enter your originating agency identifier (ORI).

   – **Username**: Enter your StateLink user name.

   – **Password**: Enter your StateLink password.

4. Click **Submit**.

   In the **Code List** area, the imported statutes are displayed.

5. If desired, to filter the code list, click **Filter Values**.

The Filter Values by city/county dialog box opens.

6. Select the filter criteria, and then click **Filter**. Multiple filter options can be selected, such as all cities, all counties, or selected cities and counties.

   The filtered statutes are displayed in the **Codes List** area.

NOTE

The filter cannot be cleared once it is applied to the code list and the changes are saved. To clear the filter, exit the Statues code list without saving the changes. If the code list values are filtered and the changes are saved, then the statutes must be imported from StateLink to override the existing code list.

---

7. Click **Save** to save the code list.

Using the Translation Management Screen

Once the state code lists are configured, use the Translation Management screen to link the code lists to the database code table values.
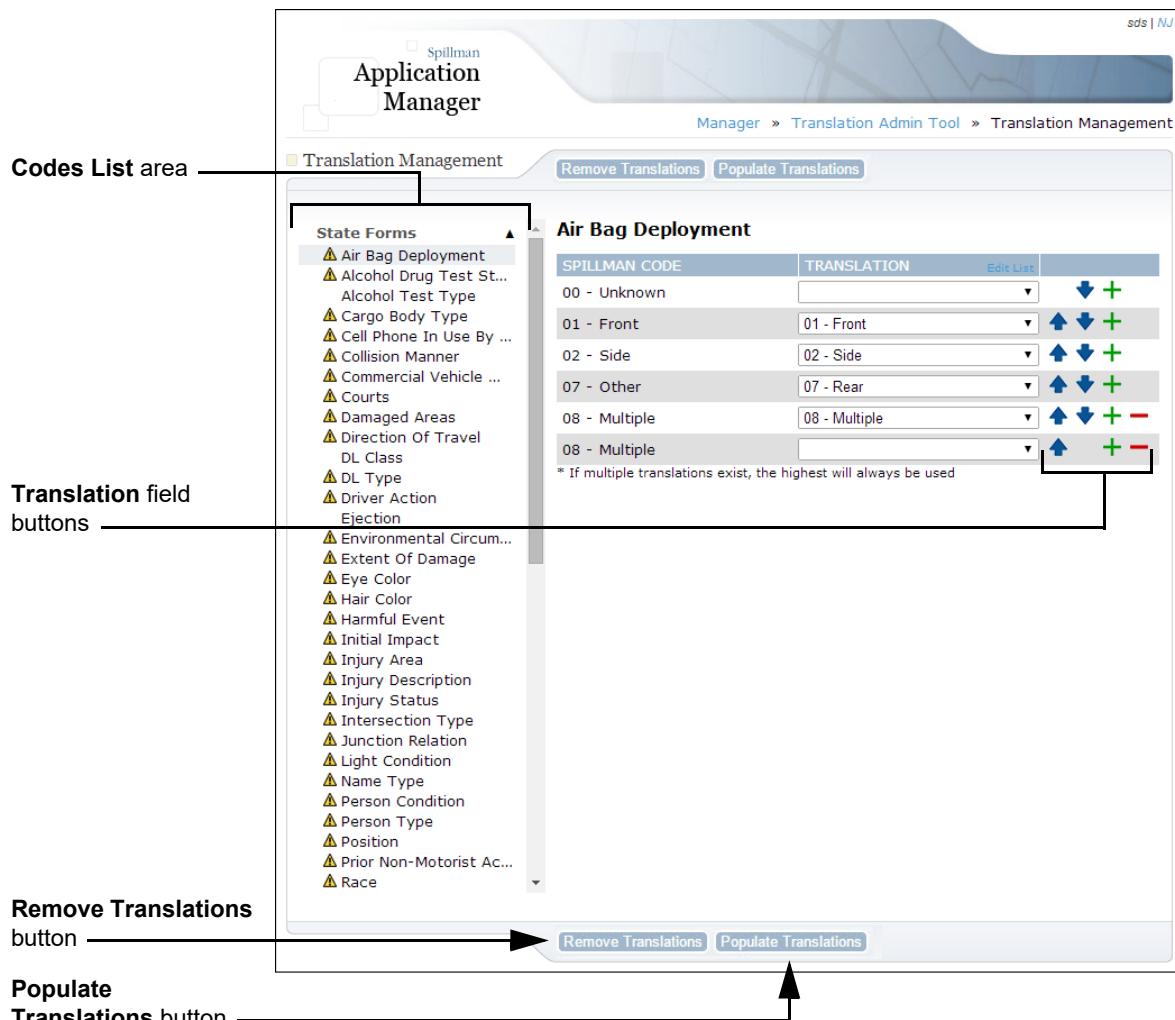
The Translation Management screen is organized into the following:

- **Code List area.** Displays the available code lists and is organized by State Form codes and StateLink codes. A caution icon indicates that there are Spillman codes with no translation values.

- **Translation column.** Displays a drop-down menu that is used to select a translation code value for the corresponding Spillman code. If there

are multiple translations for a code, then they can be moved, added, or removed by using the control icons in the far right column.

If the selected code table is large, then the **Translation** field is displayed as a filter field, instead of a drop-down menu. To display translation code values, enter at least two characters in the **Translation** field.

▪ **Spillman Code column.** Displays codes that are used in the database table, which relates to the selected code list.

Translating database codes

Use the Translation Management screen to translate database codes into state codes.

To translate database codes into state codes:

1. From the **Codes List** area, select the code list to translate.

   The database codes for the selected code list are displayed.

2. Click the **Populate Translations** button.

   State translation codes that match database codes from the Statute (Law) Codes table (`tblaw`) are populated in the **Translation** fields.

3. For each database code without a matching translation code, do one of the following:

   – If the **Translation** field is a drop-down menu, then select the desired translation code. Use the scroll bar if necessary.

   – If the **Translation** field is a filter field, then enter at least two characters of the desired translation code. The list filters as characters are entered. Select the desired translation code.

4. To add multiple translations for a database code, click the **Duplicate Row** button for that code. To remove additional translations, click the **Remove Row** button. In general, multiple translations are use only in the StateLink codes section of the **Codes List** area.

> **NOTE**
>
> Multiple translation values can exist for each database code. However, the conversion always takes whichever value is ordered the highest on the list. Therefore, use the **Move Up** and **Move Down** buttons to reorder the list as needed.

5. To remove all of the translation values in the current code list, click the **Remove Translations** button.

6. To navigate to the Code Management screen to edit the code list currently being viewed, click the **Edit List** link.

NOTE

Changes are automatically saved when a field is edited, or a button is used to add, remove, or change the order of a translation.

Using the Field Manager

The Field Manager can be used to edit fields in the tabs of the Add Record or Edit Record screens for Name, Vehicle, and Property records. The appropriate privileges are required to use this feature.
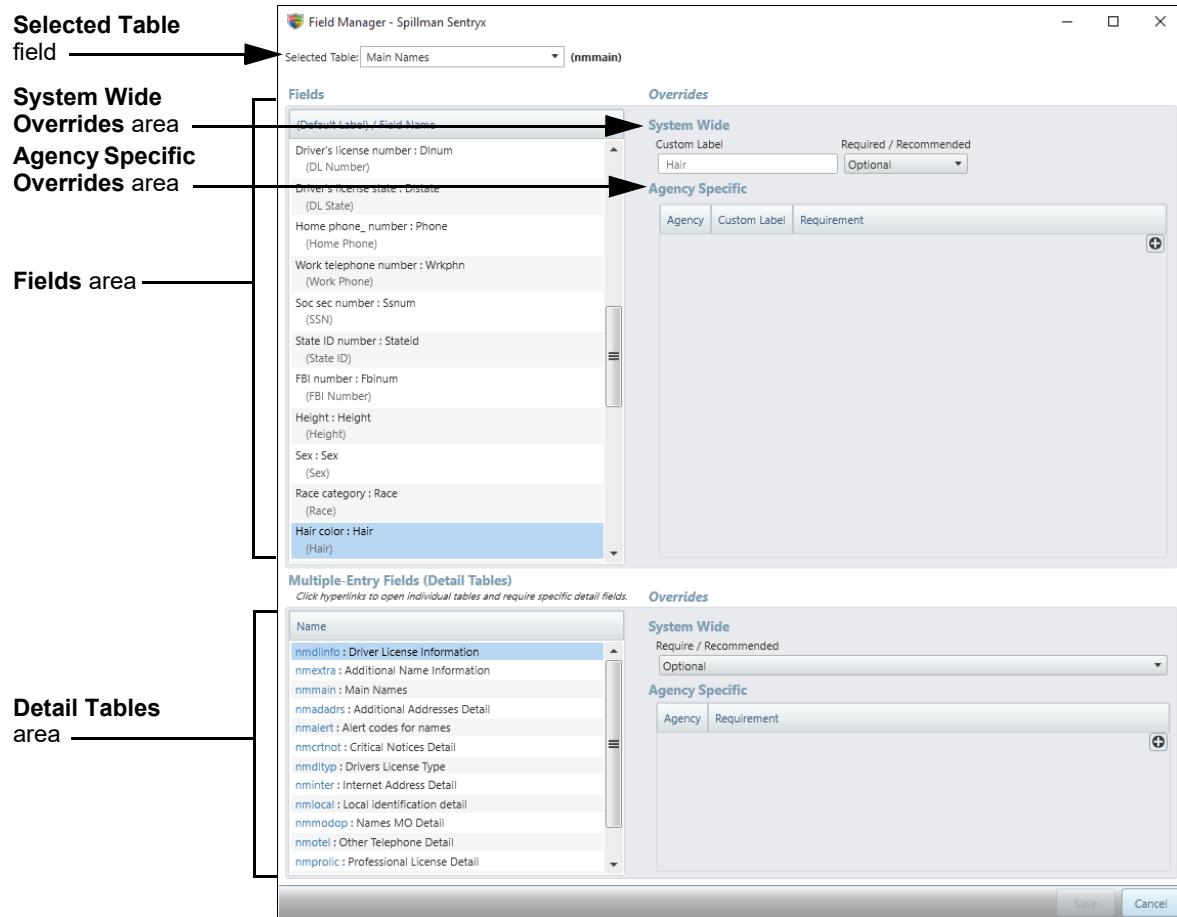
The Field Manager screen contains the following:.

- **Selected Table field.** Displays the current table in which the field is contained.

- **Overrides area.** Displays system-wide overrides for the field in the **System Wide** area, and agency-specific overrides for the field in the **Agency Specific** area.

- **Fields area.** Displays fields from the selected table.

- **Detail Tables area.** Displays fields from detail tables connected to the selected table.

Using the Field Manager to modify fields on a screen

Use the Field Manager to do any of the following:

▪ Modify field settings at a system-wide or agency-specific level.

▪ Create custom labels for fields.

▪ Set fields to `Optional`, `Required`, `Recommended`, or `Hidden`.

▪ Modify field settings for detail tables associated with the Names table (`nmmain`), Vehicles table (`vhmain`), or Property table (`prmain`).

TIP

To navigate from a detail table back to the parent table, use the drop-down list in the **Selected Table** field.

To modify fields on a screen:

1. From the desired tab on the screen right-click the field to be modified, and then click **About**.

   The About window opens.
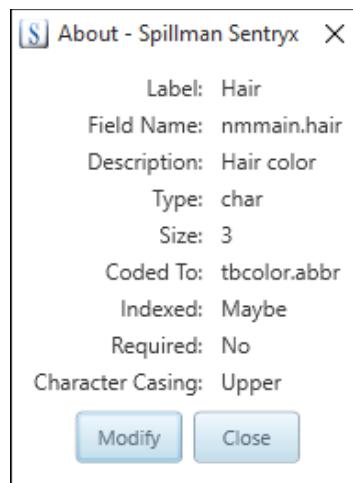
2. Click the **Modify** button.

   The Field Manager screen opens.

3. To establish system-wide settings, in the **System Wide** area, do any of the following:

   – In the **Custom Label** field, enter the new label name for the selected field.

   – In the **Required/Recommended** field, use the drop-down list to select the a field status, such as `required`.

4. To establish agency-specific settings, in the **Agency Specific** area, do the following:

   – Click the **Add** icon.

   – In the **Agency** field, use the drop-down list to select an agency.

   – Do any of the following:

      – In the **Custom Label** field, enter the new label name for the selected field.

      – In the **Requirement** field, use the drop-down list to select the field status, such as `required`.

5. Click **Save**.

   The system returns to the originally selected tab.

NOTE

To display a field after it has been set as `Hidden`:

   1. Open the Field Manager from any field.

   2. Select the table for the screen.

      – For Names, select Names table (`nmmain`).
      – For Vehicles, select the Vehicles table (`vhmain`).
      – For Property, select the Property table (`prmain`).

   3. Select the field from the appropriate field area.

   4. From the **Require/Recommended** field, select a different value from the drop-down list.

Chapter 3

Maintaining Mobile

Jump to topic:

Monitoring the Use of Mobile

Set up the User Access Log to monitor the use of Mobile by specific users or groups of users. This feature can help confirm suspected misuse or inappropriate use of the Mobile software.

The following actions can be monitored:

- Performance of queries from the Mobile Names, Vehicle, Property, and Premises screens.

- Viewing of Name, Vehicle, Property, and Premises Information records.

- Viewing of involved records.

- Viewing of photos.

Each time a user performs a monitored action, the software adds an entry in the System Log table (`sylog`) in your agency's database.

The log entry includes the following information:

- The username for the user who performed the action.

- The ID number assigned to that user's computer. If the user performed the action from the Mobile software, then the ID number is the computer's vehicle ID or IP address.

- The date and time the log entry was added.

- The table accessed by the user.

- The action performed in the table.

- Any information logged by the software, such as the search criteria used for a query.

For example, if a user searches for the Name records of all persons whose last name is Flutie, then the log entry provides the search criteria used.
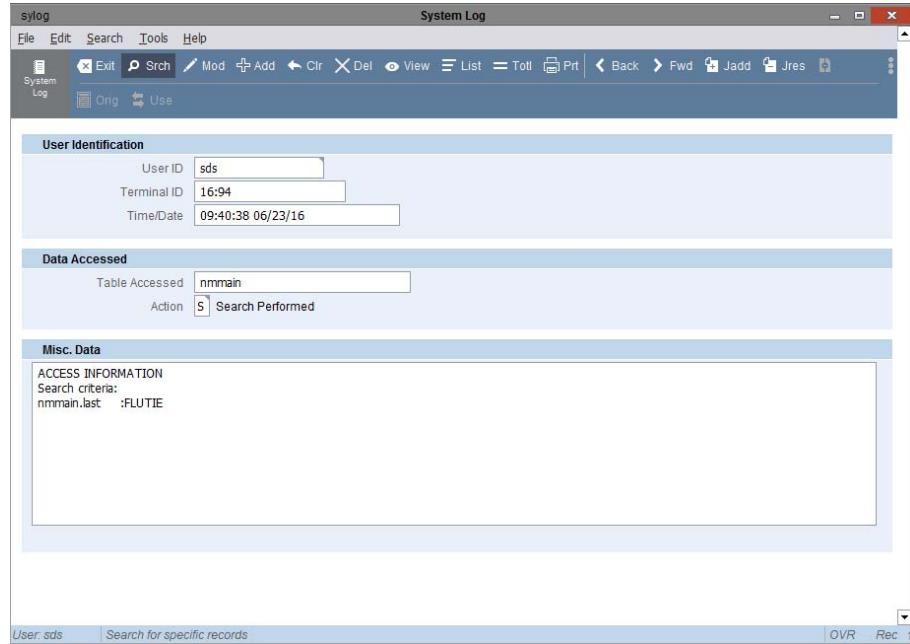
To set up which users and actions to monitor, use the `lognames` and `logmodes` parameters in the System Parameters table (`syparam`).

▪ In the `lognames` parameter, specify the users and groups of users to monitor. For more information, see the *Application Setup and Maintenance Manual*.

▪ In the `logmodes` parameter, specify the actions to monitor. For more information, see "Specifying actions to monitor in Mobile" on page 151.

> **TIP**
>
> Be selective about the users, tables, and actions that are monitored. If *all* actions in *all* tables for *all* users, are monitored, then there might be several hundred log entries created after one day of monitoring.

Specifying actions to monitor in Mobile

The `logmodes` parameter specifies the actions and tables to monitor. For Mobile, actions in the Names, Vehicle, Property, and Premises screens can be monitored.

Enter the actions to monitor. Each action has a one-letter action code. The following table describes the action codes that apply to Mobile. For more information, see the *Security Setup and Maintenance Manual*.

Use this action code	To monitor
I	The viewing of involved records in Flex and Mobile. In Mobile, the involvement must be to a Name, Vehicle, Property, or Premises Information record.
R	The viewing of records and photos in Mobile. Action code R does not apply to Flex. A log entry is added for each record that a user views. A additional log entry is added if the user opens the **Photo** tab to view the thumbnail image.
	In general, a user must select the **Photo** tab to view the thumbnail image associated with a record. However, if the **Photo** tab is active when a user opens a record, then the thumbnail image is displayed without selecting the **Photo** tab. In this case, a log entry is added for viewing the record, and another a log entry is added for viewing the photo.
	NOTE: If the user views a record multiple times while the search set is active, then only one log entry is added for that record.
S	The performance of queries from Flex and Mobile. In Mobile, the software monitors the performance of queries in the Names, Vehicle, Property, and Premises screens.
all	All actions performed in Flex and Mobile.
	NOTE: The action code all includes action codes I, R, and S, as well as action codes that apply only to the Flex software.

Viewing and printing log entries

View and print log entries from the System Log screen (`sylog`). For more information on using the System Log screen, see the *Security Setup and Maintenance Manual*.

Maintaining the Messenger Module

The following sections describe how to maintain user records in the Messenger Users table (`msuser`) and check message logs in the Messenger log table (`mslog`):

- "Deleting a Message User record" on page 153
- "Checking message logs" on page 154
- "Archiving and deleting mslog records" on page 155

Deleting a Message User record

If a user has privileges for the Messaging module, then a record is created for that user when the user logs on to Mobile. The records are stored in the `msuser` table.

To delete a Message User record:

1. At the command line, enter **msuser**.

    The Messenger Users table opens.
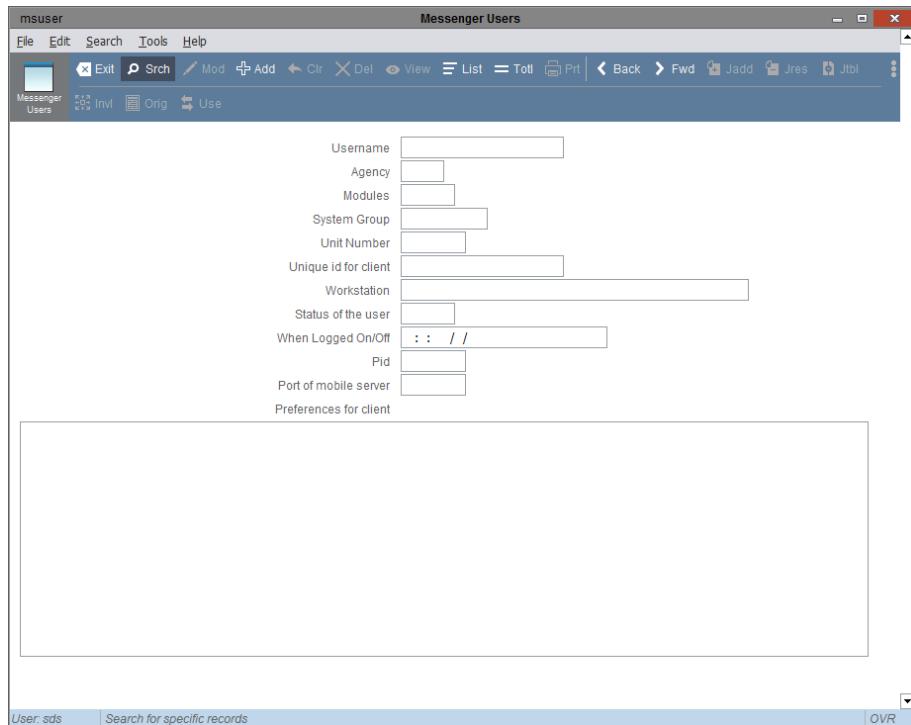
2. Search for the record to delete.

3. With the correct record displayed, click **Delete**.

Checking message logs

All messages sent using the Messaging module are logged on the server. Check the message logs for email messages, instant messages, and alert messages in the Messenger log table (`mslog`).

To check message logs:

1. At the command line, enter **`mslog`**.

   The Messenger log table opens in Search mode.
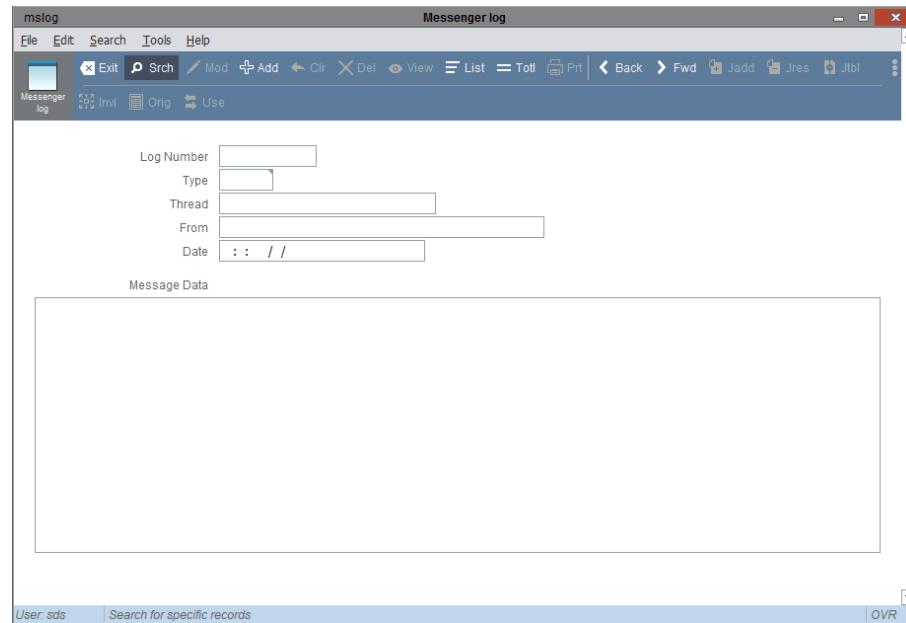
2. Enter your search criteria.

3. Click **Accept**.

The first record in the search set is displayed.
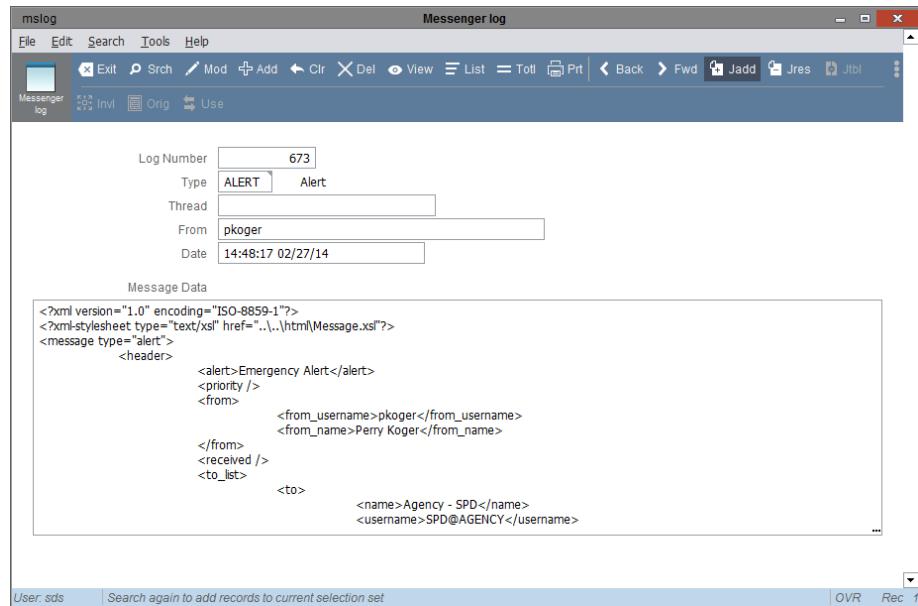
The record displays the message header, the username of the person who sent the message, the time and date the message was received, the username of the person who received the message, and the contents of the message.

Archiving and deleting mslog records

Use the Dump Mobile mslog Records report (`rpmsdump`) and the Delete Mobile mslog Records report (`rpmsdel`) to maintain the Message Log table (`mslog`). Run both of these reports regularly to archive and delete `mslog` records from the `mslog` table.

To archive and delete `mslog` records:

1. At the command line, enter **rpmsdump**.

The Dump Mobile mslog Records report screen opens.
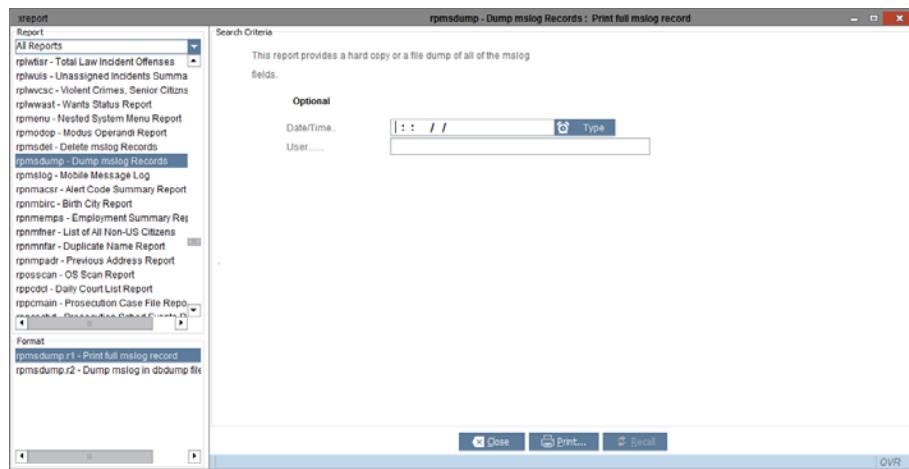
2. Enter search criteria to indicate the log entries to archive.

   No search criteria are required. However, it is recommended to enter a date range to limit the report. Otherwise, the report takes a long time and uses a large amount of memory.

3. In the **Format** area, select one of the following formats:

   – To dump `mslog` records into a standard report format recommended for hard copy printouts, select `rpmsdump.r1`.

   – To dump `mslog` records into a file for later use, select `rpmsdump.r2`. This format is recommended for tape archival. Specify a file as the destination, and then save the file to backup media at a later time.

4. Click **Print**.

   The Print dialog box opens.

5. Click **Print** to dump the `mslog` records.

6. To run the Delete Mobile mslog Records report, at the command line, enter **rpmsdel**.

7. Enter the same search criteria as in step 2.

8. In the **Format** area, select `rpmsdel.r1`.

9. Click **Print**.

   The Print dialog box opens.

10. Click **Print** to delete the specified records from the Message Log table.

Troubleshooting Mobile

If Mobile is not working properly, then determine whether your Mobile Data Computer (MDC) is communicating with the network. The following section lists the network utilities that can be used to check your MDC's network connection. If your network connection is not intact, then contact your communications provider.

If your network connection is intact but Mobile is not working properly, call Spillman Technical Services.

Running network utilities

Use the ping and traceroute utilities to check your network connection. If running one of these utilities reveals an interruption in your network connection, contact your communications provider.

Running the ping utility

The ping utility checks for a network and verifies whether the MDC is connected to the network. If your network connection is intact, then the ping utility can be run from your server to your Mobile laptop computers and client PCs, or vice versa.

Running ping from your server

To run ping from your server:

1. Access the server prompt.

2. Enter the command in the following format:

   `ping IP-address`.

   For example, enter `ping 166.128.252.249`.

   One of the following occurs:

   – If the network connection is intact, then information similar to the following example is displayed:

```
$ ping 166.128.252.249
PING 166.128.252.249: 64 byte packets
64 bytes from 166.128.252.249: icmp_seq=0.
time=497. ms
64 bytes from 166.128.252.249: icmp_seq=1.
time=559. ms
64 bytes from 166.128.252.249: icmp_seq=2.
time=511. ms
64 bytes from 166.128.252.249: icmp_seq=3.
time=511. ms
```

```
----166.128.252.249 PING Statistics----
5 packets transmitted, 4 packets received, 20%
packet loss
round-trip (ms)  min/avg/max = 497/519/559
```

– If the network connection is not intact, then your screen remains blank or an error message appears.

3. Press Ctrl+C to quit.

Running ping from a computer

To run ping from a computer:

1. From the Start menu, select **All Programs** > **Accessories** > **Command Prompt**.

   The command prompt opens.

2. At the command prompt, enter a command in the following format:

   ping IP-address

   For example, enter **ping 166.128.252.249**.

   One of the following occurs:

   – If the network connection is intact, then the utility pings four times and quits.

   – If the network connection is not intact, then a blank screen is displayed or an error message appears.

> **TIP**
>
> For a continuous ping, use the following format:
>
> ```
> ping -t IP-address
> ```
>
> To specify the number of milliseconds between the pings, use the following format:
>
> ```
> ping -w xxxx IP-address
> ```
>
> For more information on the ping command, refer to your Windows user documentation.

Running the traceroute utility

The traceroute utility traces the network connection between your computer and an IP address. If your network connection is intact, then the connection from your server to your Mobile laptop computers and client PCs can be traced, or vice versa.

**Running the
traceroute utility
from your server**

To run traceroute from your server:

1. Access the server prompt.

2. Enter a command in the following format:

   `traceroute IP -address`

   For example, enter **`traceroute 161.181.293.64`**.

   – If your network connection is intact, information similar to the
   following is displayed on your screen:

   ```
   #traceroute 161.181.293.64
   Tracing route to 161.181.293.64 over a maximum of
   30 hops
     1    552 ms      *       542 ms   155.173.8.12
     2    403 ms    485 ms    476 ms   155.173.8.1
     3    436 ms    474 ms    484 ms   155.173.9.116
     4    550 ms    592 ms    641 ms   155.173.240.174
     5    548 ms    574 ms    583 ms   161.181.293.64
   Trace complete.
   ```

   – If the network connection is not intact, then your screen remains
   blank or an error message appears.

   Traceroute exits automatically.

**Running the
traceroute utility
from a computer**

To run traceroute from a computer:

1. Open the command prompt. From the Start menu, select
   All Programs > **Accessories** > **Command Prompt**.

2. At the command prompt, enter a command in the following format:

   `tracert IP-address`

   For example, enter:

   `tracert 166.128.252.249`

   – If the network connect is intact, then connection information is
   displayed on your screen.

   – If the network connection is not intact, then a blank screen is
   displayed or an error message appears.

   Traceroute exits automatically.

Running the Mobile utilities

The Mobile utilities start and stop Mobile and display Mobile's status.

Starting or stopping Mobile

To start or stop Mobile:

1. Log in to Flex.

2. At the command line, enter **sydgmgr**.

   The Daemon Group Manager screen opens.

3. Search for the Mobile daemon group record.

4. In the correct record, from the screen toolbar, do one of the following:

   – To start Mobile, click **Start**.

   – To stop Mobile click **Stop**.

   When Mobile is started, the port on which Mobile listens must be free of connections. If users are connected to the port when Mobile is stopped, then it takes some time for the server to disconnect users from the port. When Mobile is restarted, the server tries for two minutes to establish itself on the port. This is usually enough time for all users to be disconnected. If the server does not connect to the port in two minutes, then wait a few minutes and try starting Mobile again.

Obtaining connection status for UNIX and Linux

The Mobile utilities are located in the `$MOBILEDIR/mobile/bin` directory. To run them, log in as `root`, shell out to the server, and make `$MOBILEDIR/mobile/bin` your working directory.

Obtaining connection status between servers and clients

To obtain the status of the connection between the servers and the clients, enter the netstat command in the following format:

`netstat -an | grep port-ID`

For example, if the port ID is 22630, then enter the following:

`netstat -an | grep 22630`

The server's state should be listed as `LISTENING` on local port 22630. Each client's state should be listed as `ESTABLISHED` on local port 22630.

Obtaining Mobile's connection status

To obtain Mobile's connection status:

1. Log in to Flex.

2. At the command line, enter **sh**.

3. At the UNIX prompt, enter the following:

```
cd $MOBILEDIR/mobile/bin
```

4. Log in as root.

5. At the prompt line, enter **/mblstat**. The **-p** *port* or **-f** options can also be specified.

   - **-p** *port*: Where *port* is the server port to query. By default, all ports are queried. To specify a port, enter the port ID.

   - **-f**: Provides detailed information about each of the clients connected to Mobile server and prints out vital information, such as user, client ID, status, client version, and PID.

     When the **-f** option is used, the command also deletes client files and debug files that are older than 14 days.

   The screen displays a summary of the status of the Mobile server and Mobile clients.

Obtaining connection status for Windows

The Mobile utilities are located in the `cd %MOBILEDIR%/bin` directory.

Obtaining connection status between servers and clients

To obtain the status of the connection between the servers and the clients, enter the netstat command in the following format:

```
netstat -an | grep port-ID
```

For example, if the port ID is 22630, then enter the following:

```
netstat -an | grep 22630
```

The server's state should be listed as LISTENING on local port 22630. Each client's state should be listed as ESTABLISHED on local port 22630.

Obtaining Mobile's connection status

To obtain Mobile's connection status:

1. Access the server prompt.

2. At the server prompt, enter the following:

   ```
   cd %MOBILEDIR%/bin.
   ```

3. At the prompt line, enter **/mblstat**. The **-p** *port* or **-f** options can also be specified.

   - **-p** *port*: Where *port* is the server port to query. By default, all ports are queried. To specify a port, enter the port ID.

   - **-f**: Provides detailed information about each of the clients connected to Mobile server and prints out vital information such as user, client ID, status, client version, and PID.

When the **-f** option is used, the command also deletes client files and debug files that are older than 14 days.

The screen displays a summary of the status of the Mobile server and Mobile clients.

Enabling logging

Spillman Technical Services uses logging to help troubleshoot problems with your Mobile software. Enable logging only if instructed to do so by Spillman Technical Services. When logging is enabled, your tasks are logged in a file named Mobile.log in your Mobile applications folder.

To enable the Logging option:

1. From the menu bar, select **File> Options**.

   The Options dialog box opens.

2. Click the **Logging** tab.

3. Select the **Enable Logging** check box.

4. Click **OK**.

Upgrading Flex

When upgrading Flex, stop Mobile before starting the upgrade. For more information, see "Starting or stopping Mobile" on page 160. After the upgrade is completed and the directory structure is restored (the $MOBILEDIR directory exists), restart Mobile. For more information, see "Starting or stopping Mobile" on page 160.

Training users on Mobile

The Practice database can be used for training Mobile users. To do this, set the $FORCEDLIST environment variable to the appropriate directory or directories prior to starting.

To use the Practice database and the Live database at the same time, assign each database its own port number. When changing a port number, make sure to change it on both the client and the server.

If your agency uses only one database at a time, then the port numbers can be the same.

Appendix A

Appendix A contains information about how to set up the Verified Entry feature, if your agency determines the feature is needed. For most agencies, this feature is not necessary.

The Verified Entry feature is used to defer the advanced search that Mobile preforms to validate new records against existing records. Validation can be completed at a later time, such as in the office after patrol, or by a records clerk.

> **CAUTION**
>
> Failure to validate records in a timely manner will result in inaccurate or duplicate data in your database.

Setting up the Verified Entry setting

The following setting needs to be set up for Verified Entry. The file location of the setting depends on the privilege level at which it will be set. For more information, see the following:

Setting	Description	Value
IsVerifiedEntryEnabled	Determines if the Verified Entry feature is used when records are added to Mobile. This setting can be set at the World, Agency, Group, or User level. • Set to **True** to defer validating new records until a later time. • Set to **False** to validate records at the time the record is added.	True/False

Setting up Verified Entry at the World level

To set up Verified Entry at the World level:

1. Access the Master Configuration (options.xml) file. For more information, see .

2. Search for the `<IsVerifiedEntryEnabled>` tag.

3. To defer validating records until a later time, change the value between the beginning and ending tags to **`True`**.

4. Save a copy of the file to the uclient to avoid overriding changes when patches are applied.

Setting up Verified Entry at the Agency, Group, or User level

The instructions for setting up Verified Entry at an Agency, Group, or User level depend on your operating system.

▪ For Windows, see .

▪ For UNIX or Linux, see .

Instructions for Windows

For Windows, to set the Verified Entry setting at the Agency, Group, or User level, add the setting to the properties file for the desired agency, group, or user.

To add the setting to the properties file:

1. Navigate to the following directory:

   `mobile_install_dir``/conf/mobileserver`

   where *`mobile_install_dir`* is the Mobile installation directory for your agency.

2. Do one of the following:

   – Open the properties file for the agency, group, or user.

   – If no properties file exists for the agency, group, or user, then create a properties file and open it. The file should be named using the following structure:

     – For an agency, use *`agencycode`*`.properties`, where *`agencycode`* is the code for the desired agency.

     – For a group, use *`groupname`*`.properties`, where *`groupname`* is the name of the desired group.

     – For a user, use *`username`*`.properties`, where *`username`* is the name of the desired user.

3. In the properties file, add a new line, and then enter the following:

   `Forms/IsVerifiedEntryEnabled=true`

4. When finished, close the properties file to save it.

5. Repeat steps 2–4 for each desired agency, group, or user.

Instructions for UNIX or Linux

For UNIX or Linux, to set the Verified Entry setting at the Agency, Group, or User level, add the setting to the properties file for the desired agency, group, or user.

To add the setting to the properties file:

1. At the command line, enter `sh`.

   The Spillman Terminal Emulator Window opens.

2. At the prompt line, enter the following:

   `cd $MOBILEDIR/conf/mobileserver`

3. At the prompt line, do one of the following:

   – For an agency, enter `vi agencycode.properties`
      where *agencycode* is the code for the desired agency.

   – For a group, enter `vi groupname.properties`
      where *groupname* is the name of the desired group.

   – For an agency, enter `vi username.properties`
      where *username* is the name for the desired user.

4. In the properties file, add a new line, and then enter the following:

   `Forms/IsVerifiedEntryEnabled=true`

5. When finished, in command mode, enter `wq` to save and exit the file.

6. Repeat steps 3–5 for each desired agency, group, or user.

Setting up system privileges

The following system privileges need to be set up for Verified Entry.

System privilege	Description	Privilege
`nmmain:"ve`*agencycode*	Where *agencycode* is the agency code for which privileges are being set. Allows users to access the partition that contains unverified Name records. It is recommended to grant privileges at the Group level. • For users that need to add records, grant Add and Partition In privileges. • For users that need to verify records, grant Modify and Partition Out privileges.	Add, Partition In, Modify, Partition Out
`vhmain:"ve`*agencycode*	Where *agencycode* is the agency code for which privileges are being set. Allows users to access the partition that contains unverified Vehicle records. It is recommended to grant privileges at the Group level. • For users that need to add records, grant Add and Partition In privileges. • For users that need to verify records, grant Modify and Partition Out privileges.	Add, Partition In, Modify, Partition Out
`prmain:"ve`*agencycode*	Where *agencycode* is the agency code for which privileges are being set. Allows users to access the partition that contains unverified Property records. It is recommended to grant privileges at the Group level. • For users that need to add records, grant Add and Partition In privileges. • For users that need to verify records, grant Modify and Partition Out privileges.	Add, Partition In, Modify, Partition Out
`unverifiedall`	Allows users to view unverified records for all users and agencies in the database.	Access
`unverifiedagency`	Allows users to view unverified records for all users in their agency.	Access
`unverifiedmine`	Allows users to view unverified records that they created.	Access
`mdcadmverifentry`	Allows users to access the Unverified Records screen from Mobile.	Access

To set up system privileges for Verified Entry:

1. At the command line, enter **adminutil**.

   The Administration Manager opens.

2. If necessary, select the **System** menu group, and then select the **System Privileges** menu item to open the System Privileges screen.

3. In the **Show Privileges For** field, select **Group**. In the adjoining field that appears, select the desired group name.

4. In the **Add Custom Sypriv** field, enter the desired privilege. For example, `nmmain:"ve`*agencycode*.

5. Click the **Add Custom Sypriv** button.

   The new privilege appears in the list of privileges below.

6. Select the desired level of access for the new privilege. Use the scroll bar to find the new privilege if necessary.

7. Repeat steps 4–6 for each privilege to set up.

8. Click **Save**.

For more information on setting up system privileges, see the *Security Setup and Maintenance Manual*.

A